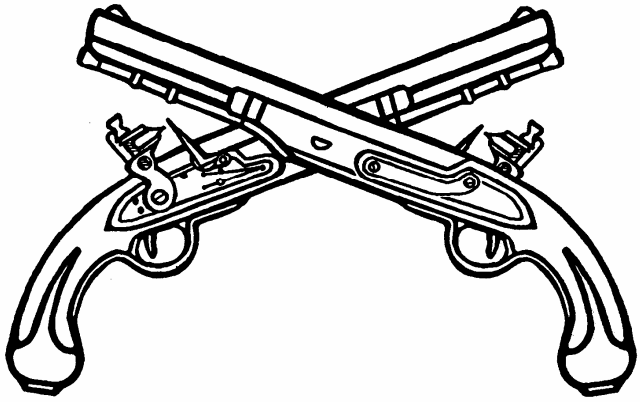
SUBCOURSE
MP2001

EDITION
B

SPECIAL MILITARY POLICE OPERATIONS

MP



SETS THE STANDARD FOR EXCELLENCE

THE ARMY INSTITUTE FOR PROFESSIONAL DEVELOPMENT

ARMY CORRESPONDENCE COURSE PROGRAM

AIPD

READINESS / PROFESSIONALISM

THRU GROWTH

SPECIAL MILITARY POLICE OPERATIONS
ADVANCED OFFICER COURSE (AOC)

SUBCOURSE NO. MP2001

EDITION B

U.S. Army Military Police School
Ft. Leonard Wood, MO 65473-8929

5 Credit Hours

Edition Date: March 1994

Subcourse Overview

This subcourse is designed to teach you the basic procedures involved in special military police operations. Contained within this subcourse are instructions on how to provide protective services, perform bomb threat contingency planning, and countering terrorist activities on military installations.

There are no prerequisites for this subcourse.

This subcourse reflects the doctrine which was current at the time it was prepared. In your work situation, always refer to the latest official publication.

Unless otherwise stated, the masculine gender of singular pronouns is used to refer to both men and women.

TERMINAL LEARNING OBJECTIVE

ACTION: You will identify procedures for: providing protective services, performing bomb threat contingency planning, and countering terrorist activities on military installations.

CONDITIONS: You will have access planning data, scenarios and necessary references.

TABLE OF CONTENTS

AR 525-13 The Army Combatting Terrorism Program, June 1992.

Use the above publication extract to take this subcourse. At the time we wrote this subcourse, this was the current publication. In your own work situation, always refer to the latest publication.

*** * * IMPORTANT NOTICE * * ***

THE PASSING SCORE FOR ALL ACCP MATERIAL IS NOW 70%.

PLEASE DISREGARD ALL REFERENCES TO THE 75% REQUIREMENT.

LESSON 1

PROTECTIVE SERVICES

Critical Tasks: 03-3761.00-1114

OVERVIEW

LESSON DESCRIPTION:

In this lesson you will learn to provide protective services.

TERMINAL LEARNING OBJECTIVE:

ACTION: Provide protective services.

CONDITION: You have this subcourse, paper and pencil.

REFERENCES: The material contained in this lesson was derived from the following publications: AR 1-4, AR 190-10, CIDR 195-10, CIDR 195-1, FM 19-10, FM 19-30, AR 195-4, AR 10-23, AR 190-14, AR 190-58, and CIDP 195-1.

INTRODUCTION

Increased incidents of terrorism, hostage taking, and kidnapping have made the mission of protection and providing security for principals extremely difficult. Preparation for these missions begins in advance of the principal's arrival and requires a long and detailed process. Military police (MP) will be heavily involved in preparing for a principal's visit to their installation.

NOTE: The "principal" is the subject of protective services missions. He is also referred to as "very important person (VIP)" and "designated person." For the purpose of convenience, the term "principal" will be used throughout the lesson.

PART A - PROTECTIVE SERVICES MISSION AND RESPONSIBILITIES OF ASSIGNED PERSONNEL

1. Mission.

The mission of the protective services is threefold:

- o To prevent any attack upon the principal.

- o To provide a deterrent to those who will be deterred by mere presence of protective services personnel.

- o To prevent the effectiveness of any attack, thereby increasing the chances of survivability for the principal. The responsibilities include protecting a principal from assassination, kidnapping, injury, and embarrassment.

2. Order.

Protective service missions are ordered for two main reasons:

- o A mission is ordered when the principal has already received a threat, or when one is implied. Consider the example of a high-ranking military officer attending a NATO conference. He may have been told his life is in danger. Even if the principal is not threatened, the situation itself implies a threat.

- o A protective services mission is ordered according to the importance of a person's office. High-ranking government officers and officials, such as the Chief of Staff of the Army, Secretary of Defense, and U.S. Ambassadors, can and usually do receive protection.

3. Goals.

Goals of Protective Services Mission

It has been shown time and time again that a protected person has a better chance of surviving an attack than an unprotected person. However, law enforcement agents agree that 100 percent security is impossible. Your job should be to reduce the chances for attack and/or lessen the amount of damage from an attack. Specifically, this includes the avoidance of:

- o Assassination - the killing of the principal.

- o Kidnapping - the taking away of the principal by force.

- o Injury - the violation of the principal's rights, especially by physical damage.

- o Embarrassment - to cause the principal self-distress.

4. Responsibilities of Preparing a Protective Services Mission.

The commander of a military installation is responsible for the safety of all distinguished persons traveling to and through his area of jurisdiction. He will normally task the provost marshal to plan and conduct a protective service operation if one is needed.

When assigned to conduct a protective services mission, remember that your primary purpose is to protect the principal from assassination, kidnapping, injury, and embarrassment.

Every phase of personal security must be planned carefully in advance. Factors to be considered in the planning phase include the importance of the protected person, political attitude of the population, obstacles involved, means of transportation, duration of the mission, geographic factors, and availability of medical facilities.

There may be sudden changes. This requires that flexibility be the keynote in planning for these missions. Weather conditions, mechanical failures, and the unexpected arrival of large numbers of visitors are three examples of ever-present potential hazards. Alternate and contingency plans must be prepared. Circumstances may cause deviation from the basic plan.

An outline of the plan could be as follows:

- o Notification of mission.
- o Planning and preparation.
  - Assignment of responsibility.
  - Receipt of itinerary, biography of their principal, and control of information contained therein.
  - Initiation of a threat collection effort.
  - Identification of logistical needs.
  - Identification of travel requirements.
  - Preparation of the operations order.
- o Execution.
  - Deployment of advance team.
  - Implement advance work.
  - Carry out mission.
- o Review.
  - Critique.
  - Preparation of after action report.

Only key personnel need a complete copy of the plan. However, the protective personnel are given a briefing on the contents of the order and should be

familiar with the whole operation. Each member commits the requirements of his specific mission to memory. Information should be restricted to as few persons as the situation allows.

During planning and the conduct of the mission, coordination between agencies involved in the mission must be close and continuous. Some of these agencies include Military Intelligence, MP, USACIDC, Explosive Ordnance Disposal, Medical, Signal, local police, FBI, and Secret Service. All available agencies should be used to learn about potential danger areas, persons, or groups. On an installation, for example, there must be coordination with headquarters commandant, transportation officer, intelligence officer, and others as applicable. Civilian authorities will include police and other interested city, county, state, or comparable officials. Whenever two or more agencies are protecting distinguished persons, the agency protecting the senior officer is responsible overall.

Much of this coordination can best be accomplished by an advance party after the official itinerary is received.

5. Basic Qualifications of Protective Services Personnel.

The persons selected to perform protective services missions are called "protective services personnel." Other terms used in this document such as "protective agents," "protective services detail," or "protective personnel" mean the same. These personnel have personal guidelines and responsibilities they must follow, as outlined below.

Performance. The protective services personnel must meet weight control standards and pass a physical readiness test as criteria for selection. The agents must also be trained in the use of assigned weapons such as the .38-caliber revolver and 9-mm pistol, the 12-gauge shotgun, and machine pistol. Failure to maintain proficiency and qualification will subject them to reassignment.

The protective team must be capable of operating any special equipment needed to accomplish the mission (for example, communications, TV monitors, or X-ray). They must also have a basic knowledge of first aid. They must currently possess and maintain qualification in cardiopulmonary resuscitation techniques.

6. Duties of Protective Services Personnel.

The protective services detail consists of various groups and members who have their own assignment and responsibilities.

Detail Leader (DL) or Special Agent-in-Charge (SAC) (for CID controlled missions). The SAC represents the next level of responsibility after the commander. He will assist in the plan development. He will be personally in charge of the specifics of the mission.

The SAC works closely with the principal's party and protective members. He handles matters with officials, press policies, public exposure, and liaison with other military and civilian agencies.

The SAC also leads the team personnel through after-action activities.

Personal Security Officer (PSO). The PSO provides close-in security of the principal. The PSO provides around-the-clock protection for the principal everywhere to include the residence while traveling. The PSO must be well-briefed, extremely well-trained, and reliable. The PSO and SAC are occasionally the same person on smaller missions. The PSOs in charge of the in-close team.

Advance Team. The advance team "clears the way" for the principal and his party. The team performs a security check at each stop along the itinerary of a principal's route before he is to use it. Any possible threats or problems are noted and dealt with as completely as possible by the security team. Close liaison with local law enforcement officials is very important. The advance team reviews air and ground traffic, personnel, locations, and anything that could affect the safety of the principal.

Protective Team. The protective team is a small unit that remains with the principal at all times. This team, along with, or subordinate to, the PSO, ensures no unauthorized persons get near the principal. They are proficient with their weapons and protective services techniques.

Residence Watch Team. The residence watch team plans for and provides security at the principal's residence. They help to select the residence if it is temporary and conduct inspections on site. They work with the advance team to review persons working at the residence. May be one or more person(s) and will maintain a written record of events (DA Form 1594).

Baggage Team. The baggage team is responsible for all personal items of the principal and his party. They are to protect the principal from theft and loss. They will prevent foreign objects or explosives from entering the principal's baggage.

7. Conduct and Demeanor of Security Personnel.

Military Police or other persons assigned to these duties are selected on the basis of their appearance, alertness, and intelligence, as well as their ability to act quickly and correctly in unforeseen circumstances. They are told that no risks are to be taken with the safety and well-being of the principals. Protective personnel, to perform their mission efficiently, must understand the terminology peculiar to an assignment of this type. Military police should know the identity of each person in the party of a protected official.

The attitude of the protected person must be estimated by the MP. In some instances, the presence of security personnel is unpleasant to a dignitary.

This is understandable in view of the lack of privacy inherent in personal security missions.

Security personnel must be aware of this natural reaction. They must anticipate it, and adhere to strict policies of nonirritating conduct. In the initial planning stages, all potential embarrassment should be avoided. It is normally good policy to avoid direct contact with the dignitary on details of arrangements. The SAC, DL, or PSO should coordinate with a member of the official party who is designated for this purpose prior to the actual start of the mission.

Restrictions on the movement of persons should be strictly enforced. Before anyone is allowed to approach the dignitary or his effects, the person is checked carefully for identification. The authority for his presence is established. Protective personnel should quickly learn to recognize all employees and regular visitors calling on the dignitary.

Access rosters should be obtained when a group of visitors is expected. Arrangements should be made with a member of the official party to identify and vouch for any unrecognized visitor.

Visitors should be admitted only at specified entrances. Control should be kept to ensure that they go directly to their approved destinations. Members of the security detail must be especially tactful and diplomatic in performing this function to avoid offending some unrecognized dignitary.

Military Police are stationed so that they can observe everyone and everything near the protected person. For example, if the dignitary is in a motorcade and MPs are lining sections of the route all will face the crowd so they can observe any suspicious actions tactfully and promptly. MPs place themselves between the protected person and any person acting suspiciously. They precede the protected person into buildings, crowded areas, or dangerous places. They also flank and follow him. Do not enter into conversation between the protected person and other persons. Information should be given only when requested. All dealings with the protected person and his associates should be on a formal basis. Never become involved with providing personal services for dignitaries or members of their parties. Attempts to ingratiate only serve to degrade the security mission. This results in a poor relationship. If the protected person or members of his party are friendly in their approach to the security detail, security personnel should react accordingly. An impersonal, businesslike approach to personal contact should be the rule.

8. Use of Weapons. There is always the danger of accidental discharge and injury of innocent persons when weapons are carried. All protective personnel must be qualified to fire the weapons with which they are armed. The numbers and types of weapons carried should be appropriate to the situation and any indicated threat based on intelligence reports of the situation and the mission. In a security mission, the weapons should be ready for use.

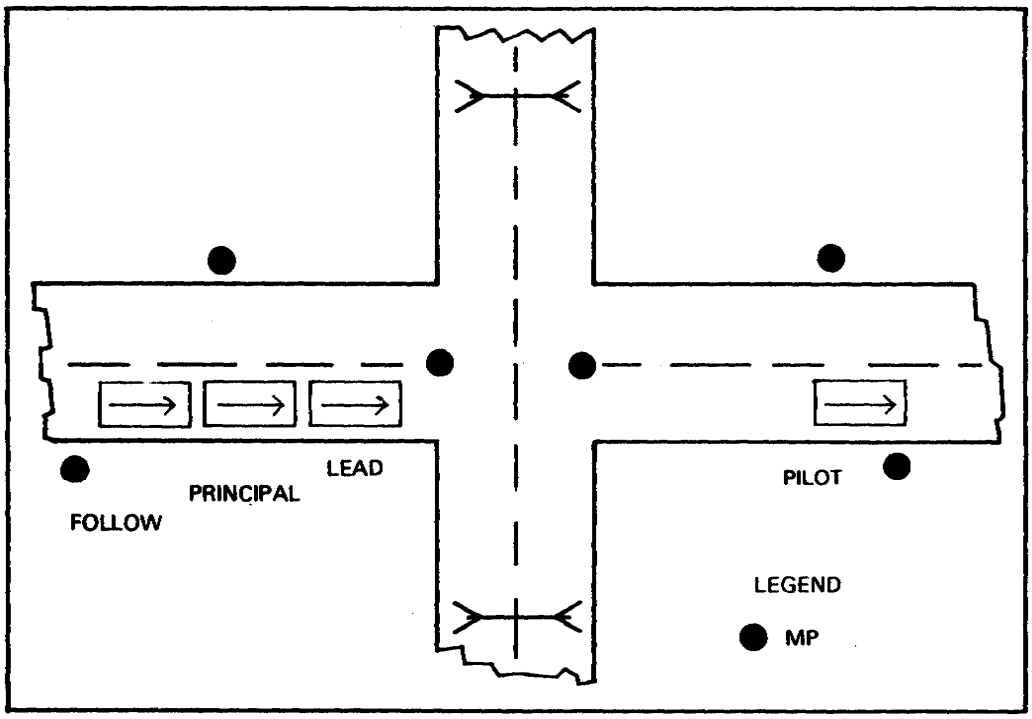


Figure 1-1. Sample MP Placement and Observation Zones.

Military Police in the protective detail should carry their assigned weapons. Semi-automatic pistols should contain a fully loaded magazine, a round in the chamber, and the safety on, if local SOP allows.

Submachine guns and folding stock shotguns, while having a place in the protective services mission, should be used only in situations where the basic principle of cover and evacuate will not work. Examples of these situations would include the principal's vehicle being disabled in the kill zone of an ambush or an attack by several assailants during a walking movement.

9. Crowd Control. Normally a principal will not be taken into an area where there is a hostile crowd. When this is unavoidable, the protective services team must concentrate on moving the principal through the crowd. Leave crowd control and apprehensions to other members of the protective service detail. (Example: Uniformed Law Enforcement).

When force is necessary, the protective service team should move with speed and surprise. At the first sign of disorder, all leaders should be

apprehended by personnel specifically assigned such duties. The real troublemakers are usually to the rear of the crowd.

The detail leader is responsible for briefing his assigned personnel on activities relating to that particular mission. These techniques are summarized below.

10. Teamwork. Protection demands teamwork. Success depends upon the cooperation and assistance of others. The failure of one person may cancel out the efforts of the whole organization. Protective personnel must be rehearsed so well that in an emergency, despite excitement and emotion, they will instinctively act correctly. They must be familiar with all phases of a protective mission. This will include the special techniques for protecting the dignitary when he is traveling by motor vehicle, train, air, boat, walking, and in public assemblies.

11. Protection While Riding in Vehicles. The type of the vehicle to be used should be considered. A closed car provides greater concealment and, therefore, provides better protection for the principal. In field environments it may be more practical for the principal to be transported in a tactical vehicle such as the HVMV rather than an armored sedan.

All automotive equipment must be in excellent mechanical condition and should be regularly inspected for signs of tampering. Drivers should be well-trained and reliable. Vehicles must be secured at all times during the security mission. A lead vehicle should precede the protected vehicle.

The follow vehicle should follow the protected vehicle as closely as possible consistent with driving safety. A pilot car should precede the convoy by about one half mile to observe hazards and report on any unusual conditions.

A spare vehicle should follow the convoy a short distance in the rear for use in emergencies. The lead, follow, and all security vehicles should maintain radio contact. The DL or PSO should be seated in the right front of the principal's vehicle.

Fixed posts at bridges, underpasses, and railroad crossings may be set: up when deemed necessary. An alternate route should be arranged for emergency requirements. Unless indicated otherwise by competent authority, the motorcade will conform with local traffic regulations. They will maintain a rate of speed consistent with road conditions.

Each situation is evaluated to determine the degree of security that is practical and necessary. The security vehicle may drop behind and follow at a discreet distance when hazards are minimal. There must be good judgment on the part of the officer in charge in solving the various situations that arise. Figure 1-2 shows a typical motorcade arrangement.

12. Travel by Train. The greatest potential security hazards often exist at the point where the protected person boards or leaves the train. Usually, this is a congested area with numerous persons carrying all sorts of bags,

packages, and containers. In a study of assassination techniques, there are a large number of attempts in this type of location. When possible, the area should be closed to the general public or the protected person should board at an isolated side. A private car may be assigned the party. It should be attached to the rear of the train. The security detail should be in control of all entrances of the car. When the train is stopped, they assume positions covering all avenues of approach to the car.

The protected person may leave the train for a temporary period. Constant security should be maintained on the train until he returns and the train departs. Prior coordination should be made with railway officials for exact scheduling of stops enroute. Railroad police and local police at scheduled stops can be contacted for standby assistance.

If needed, more security personnel may be placed in other cars of the train, seated among passengers, as an additional safeguard.

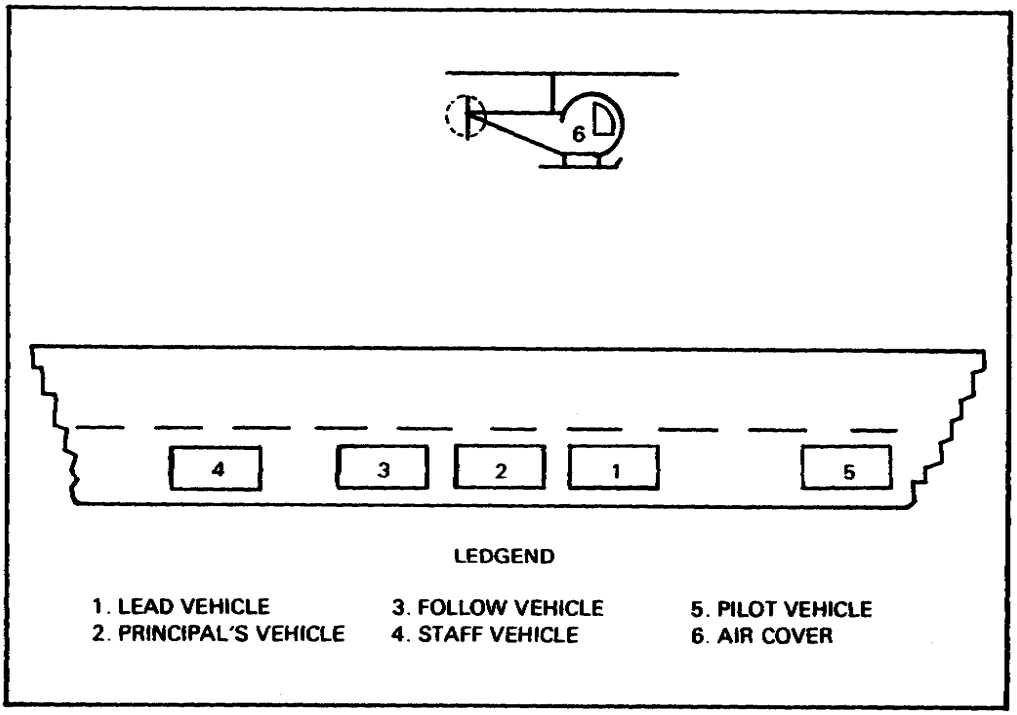


Figure 1-2. Motorcade Arrangement.

13. Travel by Air. Normally, a special plane is assigned to the dignitary and his official party. Technical safety factors such as clearance of operating personnel and control in flight are responsibilities of the operating agency when performed by the military forces. The most dangerous periods, as on trail movements, are boarding and departure times.

All structures offering observation of the boarding area should be properly secured either by closing off when not used, or by placement of a security detail. When a large crowd is expected for takeoff ceremonies, barricades and large forces of uniformed MPs and/or civilian police should be included in the planning. The place designated for the protected person should be kept under constant guard when not in use. All unauthorized persons should be kept away from contact with the plane.

When the destination is another installation, advance arrangements should be made with the local provost marshal for additional security and transportation as needed. Sufficient transportation is normally scheduled for the protected person and his party. Remember, however, that arrangements must also be made for accompanying security personnel.

14. Travel by Small Watercraft. When planning for a cruise, the boats selected should be of a type and size capable of withstanding weather and surf conditions that may be encountered. A thorough inspection of the boat designated for the protected person should be made with responsible ship personnel. The inspection is primarily for unauthorized persons stowing away and for any suspicious objects or packages. An additional check should be made for adequate lifesaving and emergency facilities. Security personnel should be alert for other craft approaching the protected person's boat. Arrangements should be made for boats to precede and follow the protected boat.

15. Protection While Walking. One of the best protective measures is varying the selection of walking times and routes. The protection team accompanying the protected person should be positioned to cover all avenues of access.

Extra security personnel should be available in the area. A security vehicle should cruise nearby. Local police agencies can be of special value in adding background security in these instances.

16. Protection at Public Assemblies. A careful search and inspection of the area should be made at the time protection is set up. A protective cordon should be set up tight around the protected person. Additional cordons should be added to the greatest possible extent. Protection in the cordon is provided by protective personnel, permanent or temporary type barricades, and a combination of the two. Screening points should be in place to admit passage of authorized persons and materials. Observant and inconspicuous security personnel should patrol among the crowd. Maximum use should be made of security aids such as floodlights and spotlights, communications, emergency equipment, special weapons, locks, barricaded areas, and bullet resistant equipment and materials.

17. Protection While in a Residence. There are three cordons of security surrounding the principal-inner, middle, and outer. The protective team occupies the inner cordon, other members of the detail occupy the middle and outer cordons with support from local MP and civil law enforcement agencies. There must be a pass system for the staff and frequent visitors. Food suppliers should be checked. Food selection and handling should be

controlled. Mail and packages should be fluoroscoped. Periodic inspections should be made of premises for safety hazards, lethal devices, and sufficiency of security equipment. Adequate communications should be maintained. All possible emergency situations should be considered. Persons providing personal or domestic services for the dignitary and his party should be screened in advance. They should receive a security briefing prior to the dignitary's arrival. This task is the responsibility of the advance party.

18. Critique and After-Action Report.

The critique is the final stage of the security mission. It is conducted so that all participants will have a clear, orderly idea of what was done properly or improperly. To improve operations, intelligent, tactful, and constructive criticism is necessary. The critique can be most effective if held as soon as practicable after the mission is completed.

The critique is so important that it must be considered a phase of the security mission itself. The effectiveness of this phase depends upon the flexibility with which the officer in charge employs it. In the critique, the officer in charge must make criticism or comments in a straightforward, impersonal manner. Participants should leave the critique with a favorable attitude toward the security mission and a desire to improve the next one. Examples of personal initiative or ingenuity, type of errors, and ways for correcting them should be covered specifically. Protective personnel should be arranged to participate in the controlled discussion. They should feel that the critique is a period for learning rather than a time set aside for criticism of their performance.

Steps in Conducting Critique. The critique cannot be planned as thoroughly as other phases of the mission. The points to be covered are influenced directly by the performance of protective personnel. Advance planning can include the time, and place of the critique, and the general outline to be followed. During other stages, the DL or PSO and supervisors can take notes to guide the critique, but detailed planning is not practical. However, the DL or PSO can ensure complete coverage of the important elements by following the general procedure below.

- Restate objective of the mission. This will enable participants to start on a common ground. This is necessary. The participants who were concerned with one aspect of the subject may have forgotten the overall objective.

- Review procedures and techniques employed. In this step, give a summary of the methods used to attain the objective.

- Evaluate the performance. This is the most important part of the critique. Using notes taken during the mission, the DL or PSO points out and discusses the strong points. Then he brings out the weaker points and makes suggestions for improvement. He must he careful not to talk down to the group. All remarks must be specific and impersonal. Personnel will not profit from generalities.

- o Control the group in discussion. The DL or PSO will discuss the points he has mentioned. He will also suggest other points for discussion.

- o Summarize. The critique is concluded with a brief but comprehensive summation of the points brought out. The DL or PSO can suggest study and practice to overcome deficiencies. The critique is business-like. It must not degenerate into a lecture.

The after-action report is a resume. It is a highlight of the security mission, written in narrative style. It is written as soon after completion of the mission as practicable.

Notes taken by supervisory personnel during operations will serve as a basis for compiling this report. Emphasis is placed upon the difficulties encountered and the procedures necessary to eliminate them.

19. Summary.

Successful conduct of a protective services mission requires careful and continual prior planning, analysis, research, and coordination. Mission responsibilities should be set early and kept under the overall supervision of a single person to ensure mission success. Each phase of the mission should be clearly defined. Coordination between responsible persons must be effective and timely to assure complete protection of the principal. The plan must also be flexible enough to cover unforeseen changes. After the mission, critiques and after-action reports are helpful in planning for future requirements.

Part B: THREAT ANALYSIS AND ITS RELEVANCE TO THE PROTECTIVE SERVICES DETAIL MEMBER

1. Threat Analysis.

Your first action as detail leader, upon receiving a protective services mission, is to develop a threat analysis. In doing so, you will find out what groups of people pose a threat to your principal and how you may best prepare for them. Factors to examine in conducting your threat analysis include active revolutionary groups in the area, previous attacks on the principal (if any), and the form in which these attacks were carried out.

2. Motivation. Although there are possible motivating factors in an attack on a person, there are some which are more common than others.

- o Revolutionary - The obsession to change or destroy a current government is a common motivating factor. The assailant's limited perspective shows him that change comes only in the form of assassinations of heads of state.

- o Economic - Belief that the principal is the cause for economic conditions is also common. The assailant may act on behalf of himself, his family, group, or nation.

- o Ideological - Sometimes ideas expressed by people in power threaten belief systems of others. If the threat is strong enough, it can be the reason for a threat or attack on the person expressing the idea. Martin Luther King, Jr had been receiving threats on his life for years before his assassination.

- o Personal - Some assassinations have been motivated by purely personal drives. These can be real or imagined. The assassin related to the victim through revenge, jealousy, hate, or rage.

- o Mercenary - In some cases, attacks have been made strictly for a monetary award.

- o Psychological - These factors tend to be complex. They seldom are the only motivating factor.

Usually, a psychological factor is present with one of the other factors listed above. An assailant with such a problem might not even be aware of the real motivating factor for his attack.

3. Group Modus Operandi. This element involves finding out how the group that poses a threat to your principal operates as a whole and their particular methods of operation. You must weigh such factors as:

- o Strength - size of group and availability of support.

- o Equipment - capability of equipment and associated firepower.

- o Training levels - group training and level of commitment.

Each group that could pose a threat to your principal usually has their own pattern of activities. This pattern made up of the above factors should be noted. Take it into account in planning your protective service mission.

4. Mass Media. To better understand the situation that surrounds your principal, you must be familiar with the media. It provides inexpensive, but valuable, information which can assist your threat analysis. Information on political climates, economics, and populace attitudes, can all affect your principal as a representative of the government. The newspaper in particular can be of great help. Not only does it provide great detail on the many potential hazard situations, but past attacks and threats on your principal or others are recorded in detail. They can be used to plan your current protective mission.

Remember to be as detailed as possible when examining such information. The more you know about possible threat groups and conditions, the better your preparation will be.

5. Using the Threat Analysis in Planning Drills.

After compiling your information, you will have a fairly clear picture of what your threats may be and methods of attack. To counteract terrorism, you must think like a terrorist. For example, if a suspect group has used motorcycles for transportation and explosives as a weapon, you must be prepared for this type of action. Drills must be performed in which members of your team act as terrorists using the modus operandi of the threat group. In this way, your team will acquaint themselves with the motives and actions of possible threat groups. They should be better prepared to repel such threats. The training should include this drill, but not be limited to it. You must still prepare to respond quickly to all possible threats to protect your principal.

The threat analysis is crucial to the planning of your protective service mission. The greater the time and effort spent in this area, the better the chance of protecting your principal from assassination, kidnapping, injury, or embarrassment.

Part C: AUTHORITY AND RESPONSIBILITY FOR PROTECTIVE SERVICES MISSIONS

1. Commander Responsibilities.

The Major Army commander exercises jurisdiction over certain geographical areas assigned by the Army. He is responsible for protective services missions as assigned. They include development of plans to ensure physical protection of Army installations. The commander is also responsible for all very important personnel that travel in his jurisdiction without their own protection. The Deputy Chief of Staff for Personnel (DCSPER) has Department of the Army (DA) staff responsibility for coordination with commanders of installations or activities for the security of distinguished persons, as appropriate.

The commander can also receive the assignment from the agency responsible for protecting the principal. The name of the title of the principal determines which agency will make the request. Thus, the written request will determine which agency is responsible for the overall protection.

2. Agency Responsibilities.

Figure 1-3 is a list of possible principals and the agency that is responsible for their overall protection.

The Special Assistant to the Secretary and the Deputy Secretary of Defense, or an authorized representative, must approve requests for U.S. Secret service support. Support is obtained from the Department of the Army. Commanders may respond to urgent requests without advance approval; however, approval on ongoing actions will be requested immediately. Persons protected by the U.S. Department of State is outlined in Figure 1-4.

- The President and members of his immediate family
- The President-elect and members of his immediate family, unless protection is declined
- The Vice President or other officer in line to succeed the President and members of his immediate family, unless protection is declined
- The Vice President-elect and members of his immediate family, unless protection is declined
- A former President during his lifetime and his wife
- The widow of a former President until her death or remarriage, unless protection is declined
- Children of a former president until they reach age 16, unless protection is declined
- Persons determined by the Secretary of the Treasury and the Advisory Committee as being major presidential and vice president candidates, unless protection is declined
- Visiting heads of a foreign visits chosen by the President, unless protection is declined
- official representatives of the United States

Figure 1-3. Persons Protected by U.S. Secret Service.

- Secretary of State
- Undersecretary of State
- Ambassadors stationed abroad
- Foreign visitors in the U.S. or a territorial possession, when directed by the President

Figure 1-4. Persons Protected by the U.S. Department of State.

3. USACIDC Responsibilities.

The Department of the Army can also provide security for all U.S. Government officials, both domestic and foreign. The Army protective role is handled by the U.S. Army Criminal Investigation Command (USACIDC). The USACIDC plans for, and conducts protective services operations for persons designated by higher authority. Primary focus is placed upon protection of the Secretary and Deputy Secretary of Defense, Secretary of the Army, and Chief and Vice Chief of Staff, U.S. Army. The protection of dignitaries other than those outlined above is normally the responsibility of the commander exercising jurisdiction over the area visited.

The USACIDC can also provide protective service support to the U.S. Secret Service, U.S. Department of State, and the Department of Defense.

Part D: PROBLEM AREAS ASSOCIATED WITH PROTECTIVE SERVICES MISSIONS

There are four distinct problem areas connected with protective services missions: personnel, expenses, equipment, and liaison requirements.

1. Personnel Requirements.

The personnel problem is twofold. The first problem is getting enough qualified people to conduct the mission. This can be attributed to a shortage of manpower assets and lack of trained Military Police.

The second problem is the conduct of personnel on the mission. Protective services personnel are always in the public eye. Their actions reflect on the principal and the Department of Army. The protective personnel protect the principal and his party. They must also present the best image possible to the public.

2. Expenses and Reimbursements.

Protective services missions generally are funded by the agency requesting the mission. Expenses for rental cars, hotel rooms, meals, and phone calls will be reimbursed. The following procedures will be used:

- Team members use actual expense allowance (itemized daily, within CONUS) or special per diem allowances (outside CONUS) in accordance with Volume I, Joint Travel Regulation.

- All other mission-related expenses are reported in accordance with AR 195-4 (Use of Contingency, Limitation .0015 Funds for Criminal Investigative Activities).

All funding requirements must be defined and documented early in the mission. You must find out the exact funding responsibilities of each agency involved. Include the Department of the Army, civil police and the host agency.

3. Equipment.

You also need to determine needs early in the mission. Each mission is different; equipment will vary. Make sure you act soon enough to assess what you need and then obtain it.

4. Liaison Requirements.

Again, this is a task you begin early in the mission. Determine which agencies can assist in your threat analysis. They will provide information on potential danger areas, persons or groups. Consider agencies such as Military Intelligence, USACIDC, and the FBI. Other agencies can assist with the actual mission. Recruit forces from the local police and the host agency. There are also agencies that provide emergency services. Connect with local medical facilities, the EOD, and other crisis response units. You must keep close and continuous contact with support agencies throughout the mission.

LESSON 1

PRACTICE EXERCISE

This practice exercise is designed to test your knowledge of the material. This lesson covered the required material to provide protective services. To check your comprehension of the lesson, complete the practice exercise below. All of the questions are multiple-choice with one correct (or best) answer. Try to answer all the questions without referring to the lesson material.

When you have answered all the questions, turn the page and check your answers against the answer key. Review any questions you missed or don't understand by referring to the corresponding reference page. When you have completed your review, continue to the next lesson.

1. You have been assigned to conduct a protective service mission. One of your goals is to provide a deterrent to those who will be deterred by the presence of protective services personnel. What is your other goal(s)?

A. To capture any and all terrorists.
B. To prevent terrorists from ever attacking the principal.
C. To lessen the effectiveness of any terrorist attack.
D. Both B and C.

2. You have assigned to certain members of the protective services mission the task of "clearing the way" for the principal. What have you formed?

A. Protective detail.
B. Residence watch team.
C. Advance team.
D. Baggage team.

3. How would you describe the motivation of a terrorist group whose goal is the overthrow of the current government?

A. Ideological.
B. Mercenary.
C. Revolutionary.
D. Economic.

4. As installation commander in Germany, you receive an order to support a protective services mission for a U.S. Ambassador. Which agency has the primary responsibility?

A. U.S. Army Criminal Investigation Command.
B. U.S. Secret Service.
C. U.S. State Department.
D. Federal Bureau of Investigation.

5. What would you consider when accounting for the expenses in your mission?

   A. The military installation will reimburse expenses.
   B. The Military Police School will reimburse expenses.
   C. Expenses are covered by the secret service.
   D. The agency requesting the mission will reimburse expenses.

LESSON 1

PRACTICE EXERCISE

ANSWER KEY AND FEEDBACK

Item		Correct Answer and Feedback
1.	D.	To prevent terrorists from ever attacking the principal. To lessen the effectiveness of any terrorist attack. To provide a . . . (page 1-2, para 1).
2.	C.	Advance team. The advance team . . . (page 1-5, para 6).
3.	C.	Revolutionary. The obsession to change or . . . (page 1-12, para 2).
4.	C.	U.S. State Department. Support is obtained . . . (page 1-15, Figure 1-4).
5.	D.	The agency requesting the mission will reimburse expenses. Protective services missions. . . (page 1-16, para 2).

LESSON 2

BOMB THREAT CONTINGENCY PLANNING

Critical Task: 03-3761-00-1112

OVERVIEW

LESSON DESCRIPTION:

In this lesson you will learn to perform bomb threat contingency planning.

TERMINAL LEARNING OBJECTIVE:

ACTION: Perform bomb threat contingency planning.

CONDITIONS: You have this subcourse, paper and pencil.

STANDARD: To demonstrate competency of this task you must achieve a minimum score of 70 percent on the subcourse examination.

REFERENCES: The material contained in this lesson was derived from the following publications: CIDR 195-1, CIDP 195-1, FM 19-30, FM 19-6, and FM 19-15.

INTRODUCTION

Bomb threat contingency planning must begin with an understanding of the psychology and technology available to the bomber. Security against bomb threats should be based on these aspects as well as the targets involved.

Several factors of individual and group psychology are operational in the mind of the bomber. Bombs have been associated in the past with revolution, anarchy, and subversive conspiracy. The planning, construction, and execution of a bombing can provide a group with satisfying feelings of conspiracy, danger, action, drama, heroism, and a revolutionary flair. Bombing is psychologically rewarding and relatively safe for the bomber. In addition, it is depersonalized violence with great potential for terror and publicity.

PART A: DISCUSS THE BOMBER

1. Technology of the Bomber.

Would-be bombers must have access to explosives, or the raw materials from which they are made. They need the knowledge to produce bombs from these

materials. This knowledge can be obtained easily by anyone. United States Army publications are the principle source of this knowledge.

The following is a list of these publications:

FM 31-20	Special Forces Operational Techniques
FM 21-50	Ranger Training and Operations
FM 19-30	Physical Security
FM 5-13	Engineer Soldier's Handbook
FM 5-25	Explosives and Demolitions
FM 20-32	Landmine Warfare
ST 31-180	Special Forces Handbook

Commercial books are another source of knowledge. Lenz's Explosives and Bomb Disposal Guide is the most well-known book. It was written to educate police bomb disposal personnel. The Anarchist Cookbook by William Powell contains recipes for explosives and know-how to make bombs, fuses, and booby traps. Advice on where these devices can be placed to do the most harm is also provided.

Extremist groups have distributed their own guides based on military and commercial publications. These guides explain the manufacture and placement of bombs. They also encourage readers to use this knowledge against targets of political significance.

Explosive material is obtained mostly by theft. Between January 1969 and May 1970, 31,370 pounds of explosives, 94,018 blasting caps, and 101,504 feet of detonation cord or fuses were stolen. In this same period, 304 M14 antipersonnel mines were stolen from a test range operated by a private research institute. The most common targets for theft are construction sites. Military installations are another source of explosives.

Explosives can be easily purchased in some places. Theft is not always necessary. Laws governing the sale and possession of explosives vary from state to state. Title IX of the Organized Crime Control Act of 1970 makes Federal crimes out of several acts, including:

- Interstate transport of explosives to cause property damage, injury, or death.
- Use of explosives to damage any Federal buildings.
- Use or carrying of explosives during the commission of a felony.
- Use of explosives to damage buildings, property, or vehicles used in interstate or foreign commerce.
- Making a bomb threat through the use of an interstate instrument, such as the mail or telephone system.

The Control Act of 1970 also attempts to license and regulate explosives when sufficient interstate contacts exist. Despite laws regulating explosives, there is little control over a would-be bomber's access to explosives. The ready access to chemicals and the simple instructions set forth in the guides mentioned above are all the technology needed by would-be bombers. Bombs are, therefore, a very serious threat. They should not be underestimated.

2. Security Against the Bomber.

It may not be possible to completely keep explosive devices out of a facility. However, an active security program will greatly increase the difficulty of the bomber.

Four security measures should be emphasized within a physical security program as control measures against the introduction of bombs. These are identification and control procedures, package and material control, intrusion detection systems (IDS), and closed circuit television (CCTV).

Identification and Control Procedures. The primary objective of these procedures is to be aware of who is entering and exiting the facility and to keep persons from wandering through the facility. This can be as complicated as automated entry control or as simple as being greeted and challenged by a receptionist. The use of single card or badge, card or badge exchange, or multiple badge systems is useful in the control and movement of persons into, within, and out of the facility. These measures serve as an obvious deterrent against a would-be bomber believing an unobserved entrance may be possible.

Package and Material Control. In conjunction with the above procedures, there should be control of packages entering a facility. Procedures which may be used are:

- A roster of expected incoming packages.
- Verification of all unexpected items prior to acceptance.
- Sign in/out sheet of persons with hand-carried items, listing the items.
- Metal detectors.
- Bomb-detector dogs.

Package control should not be limited to packages carried openly. It must include controls on articles of clothing, handbags, briefcases, umbrellas, lunch boxes, and anything of a similar nature, which can be used to hide bombs. Even a folded newspaper could carry a bomb or incendiary device.

Motor vehicles are another important potential bomb threat. All motor vehicles privately owned and operated by the site personnel should be registered with the command post. Whenever possible, parking areas for such

vehicles should be located outside the perimeter of protected areas. Entrances and exits to parking areas should be separate from others.

The following information, contained in the postal pamphlet "Bombs by Mail," should be available to all mail-handling personnel. A copy should be in each unit mail room.

- o Mail bombs may bear restricted endorsements such as "Personal" or "Private." This factor is important when the addressee does not normally receive personal mail at the office.
- o The addressee's name and/or title may be inaccurate.
- o Mail bombs may reflect distorted handwriting or the name and address may be prepared with homemade labels or cut-and- paste lettering.
- o Letter-type bombs may feel rigid or appear uneven or lopsided.
- o Parcel bombs may be unprofessionally wrapped with several combinations of tape used to secure the package and may be endorsed "Fragile-Handle With Care" or "Rush-Do Not Delay."
- o Parcel bombs may be of irregular shape or have soft spots or bulges.
- o Parcel bombs may make a buzzing or ticking noise or a sloshing sound.
- o Pressure or resistance may be noted when removing contents from an envelope or parcel.

Mail handlers that become suspicious about a package should NOT:

- o Open the article.
- o Put it in water or a confined space like a desk drawer or a filing cabinet.

Instead they SHOULD:

- o Isolate the mailing, then evacuate the immediate area.
- o If possible, open windows in the immediate area to help vent potential explosive gases.
- o Ignore the possibility of embarrassment if the item turns out to be innocent. Contact the nearest EOD, Military Police, or postal inspector for professional assistance.

3. Suspicious Items.

Employees must be able to quickly determine if a suspicious item belongs in an area. The only way to do this is to keep clutter to a minimum. All personnel

must be able to quickly scan their immediate areas and identify anything out of the ordinary. Training will teach personnel to know that if a suspected device is discovered, they SHOULD NOT touch the device. Instead, they should ascertain that it doesn't belong, make sure no one touches it, and report the discovery to a supervisor or security officer.

4. Ground Maintenance.

The following procedures should be considered in planning the outside layout of the activity.

- o Reduce or eliminate shrubbery and vegetation next to the building to remove a natural hiding place.
- o Move dumpsters away from the facility into concrete block areas to eliminate a prime hiding spot.
- o Restrict parking areas next to the building and report, inspect, remove, and monitor apparently abandoned vehicles.
- o Eliminate or reduce parking with protected areas like underground garages, internal tunnels and passageways.

5. Security Education.

Personnel must be made aware of the possibility of a bomb threat or a bombing incident. They should view unidentified persons as trespassers. They should be encouraged to report things that "may be nothing," but are out of the ordinary. It is essential to make all personnel part of the security team.

Part B: BOMBING TARGETS AND BOMBING MOTIVES

1. Bombing Targets.

According to the National Bomb Data Center, residential property, at which three of every ten bombings in 1987 were directed, continues to be the most frequent bombing target. Vehicular bombings accounted for nineteen percent of all incidents. Commercial operations were the targets in fourteen percent, and postal facilities and equipment in five percent.

Closely following residences as bombing targets are commercial buildings. Significant percentages of bombings also occur in vehicles and schools.

2. Bombing Motives.

Bombing targets are closely related to bombing motives. The two top motives for bombing according to the NBDC are malicious destruction and personal hate. These are non-political reasons. Those involved would be likely to pick the easiest targets.

Non-political Motives. Bombing has often been used as a method for homicide, intimidation, harassment, and revenge. Bombings can be used to put a competitor out of business or to get even with management in labor disputes. Monetary gain through ransom or merely destroying evidence at a crime scene are other non-political motives. Many bomb threats are rooted in the psychological disorders of the perpetrator.

Political. Some bombings are designed to stop or impede government operations by destroying records and interrupting normal operations. Other bombings are more symbolic. They are used to demonstrate opposition to a political cause. The bombing is used as an avenue to publicity that might not otherwise be available. The bombing can serve the dual purpose of interfering with an activity and calling attention to the political motives of the bomber. Political bombings tend to avoid personal injury so as to not adversely affect their public image.

The most serious form of political bombing is that related to terrorism. The aim of terrorism is to promote fear in the populace and to make them lose faith in the government. Terrorists are not interested in maintaining a good image. Therefore, injury and death are often a part of their bombing activities.

Unfortunately, bombings may also be contagious. Other groups of persons may take up where the original group left off.

3. Summary.

Despite the growth of Anti-establishment feelings in the 60's and early 70's, bombers motives have stayed pretty much non-political. Bombings of military facilities and related communications and transportation facilities, though fewer in number, are more likely to be politically motivated.

Part C: BOMB THREAT CONTINGENCY PLANNING

1. Telephone Procedures.

The first moments of a bomb threat can be crucial to the evaluation of an incident. It is important to obtain as much information from the threat source as possible. The person receiving the bomb threat should attempt to get as much information as possible from the caller.

When a telephone bomb threat is received, one or both of the following are occurring:

- Someone has actual knowledge that a device has been planted.
- Someone wishes to disrupt an operation (pranksters).

Noting what is said, and how it is said during a bomb threat call can help determine which of these is true. The person receiving the call may be the only one to have contact with the bomber. It is, therefore, important that

those people most likely to receive bomb threat calls be aware of correct telephone procedures.

During an actual bomb threat call, the receiver tends to be highly excited. Proper training must provide the receiver with the ability to remain calm and be able to pick out the important facts.

Bomb threat phone call checklist should be readily available and filled out by the receiver (see Figure 2-1). FBI Form 6-136 (Bomb Threat Checklist) is recommended by DA Pam 190-52. This is the right size to fit under a phone. Other checklist may be used (see Figure 2-2) or a locally produced checklist can be developed.

The exact wording of the bomb threat should be written down. For example, if the caller says, "Specialist Smith, there is a bomb planted on your floor. You and your six co-workers have 20 minutes to clear out," the receiver must note all that information. Otherwise, valuable evidence will have been lost.

The receiver must note the exact date and time of the phone call. This may prove important in discovering the location of the call. The receiver should attempt to elicit from the caller the following information:

- The exact location of the bomb.
- The type of bomb.
- The type of explosives used.
- The description of the device.
- The reason for the bombing.
- Name and location of the caller.
- The time the device will detonate.

The caller may describe what the bomb looks like, how it operates, and its general characteristics. This is what is known as a descriptive bomb threat. A descriptive bomb threat is often likely to be real.

The person making a bomb threat call could reveal enough information about himself for the receiver to later identify him. For this reason, it is very important to keep the caller talking as long as possible. This also increases the possibility of tracing the phone call.

Attempt to determine the sex, age, and mental attitude of the caller. Note any peculiarity of accent. Note any background sounds. They may prove helpful in determining the caller's location.

If time permits, ask the caller who he is and where he is. In some instances, the caller may unthinkingly reply.

Working arrangements may allow for signaling another employee to listen in on the call. This should be planned. The second person can concentrate on characteristics of the caller and background sound. The primary receiver can concentrate on the exact words of the caller.

2. Notification of Support Agencies.

As a rule, those agencies that should be notified are:

- o Military Police.
- o Explosive Ordinance Disposal (EOD).
- o Fire Department.
- o Medical personnel.
- o Other persons as dictated by local SOP. These might be higher commanders, public affairs personnel, or staff duty personnel, or emergency operation center (EOC).

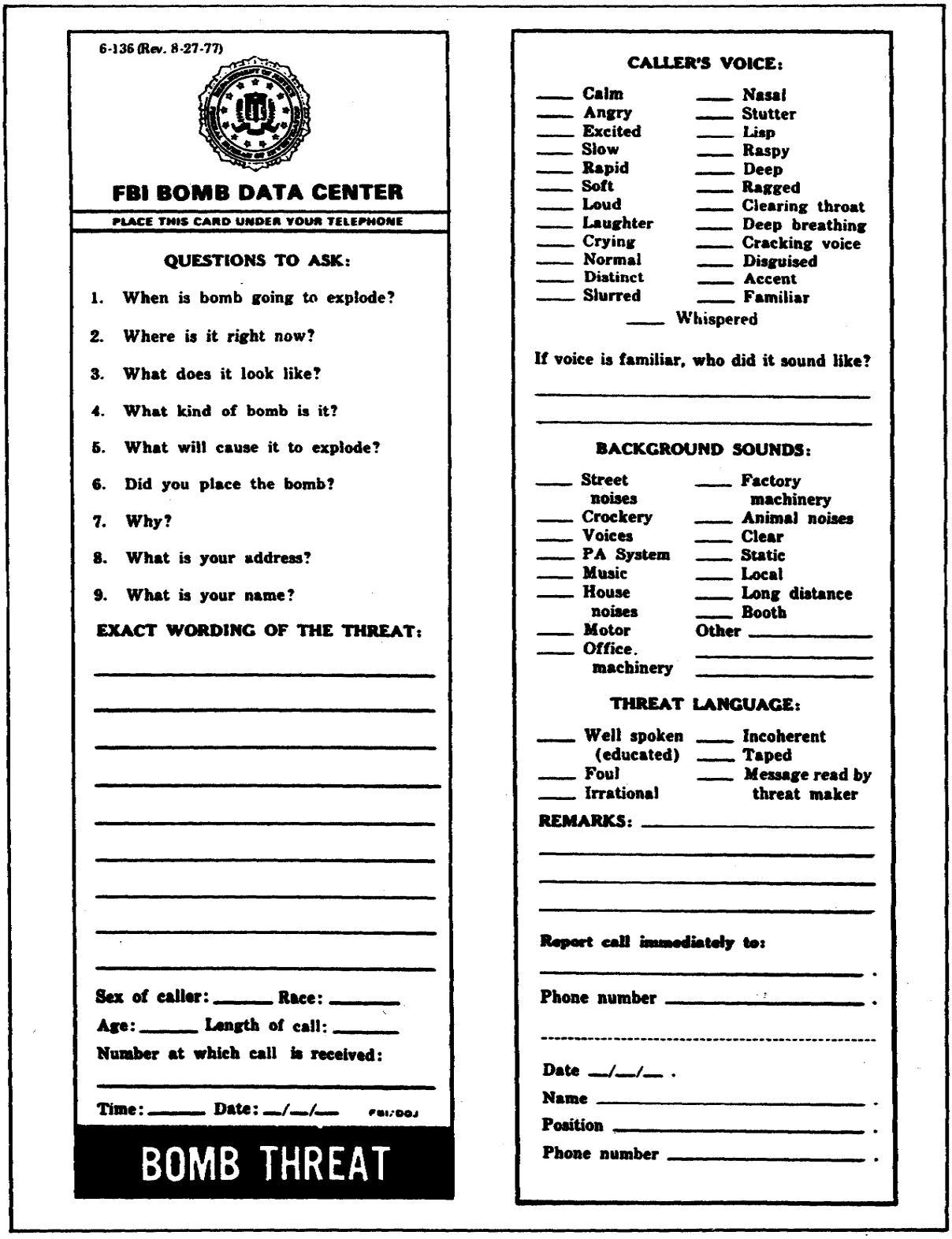
In addition, local police, the FBI (when the threat falls within their jurisdiction), and public utilities may also be notified.

Any person in a position of responsibility must be briefed on each notification to be made and its priority.

Military Police (MP). Normally, the MP desk sergeant is the first person who is notified. Depending on local station SOP, he would make the necessary notifications. In some locations, it might be the duty of the persons in the building to make the notifications. Prior planning must determine who is responsible.

MP will respond as the initial investigating agency for a bomb threat. They will cordon off the target area, provide traffic control, and obtain facts for the investigation. They will NOT conduct a search as they will not be familiar with the search area.

Explosive Ordinance Disposal (EOD). Normally, EOD personnel will not respond to a bomb threat unless a suspicious item is located. They may be able to tell you if any other threats have been received of a similar nature, and if any bombs were discovered. They may also give guidance if a device is located.



6-136 (Rev. 8-27-77)

FBI BOMB DATA CENTER

PLACE THIS CARD UNDER YOUR TELEPHONE

QUESTIONS TO ASK:

1. When is bomb going to explode?
2. Where is it right now?
3. What does it look like?
4. What kind of bomb is it?
5. What will cause it to explode?
6. Did you place the bomb?
7. Why?
8. What is your address?
9. What is your name?

EXACT WORDING OF THE THREAT:

Sex of caller: _____ Race: _____

Age: _____ Length of call: _____

Number at which call is received:

Time: _____ Date: __/__/__ FBI/DOJ

BOMB THREAT

CALLER'S VOICE:

____ Calm	____ Nasal
____ Angry	____ Stutter
____ Excited	____ Lisp
____ Slow	____ Raspy
____ Rapid	____ Deep
____ Soft	____ Ragged
____ Loud	____ Clearing throat
____ Laughter	____ Deep breathing
____ Crying	____ Cracking voice
____ Normal	____ Disguised
____ Distinct	____ Accent
____ Slurred	____ Familiar
____ Whispered	

If voice is familiar, who did it sound like?

BACKGROUND SOUNDS:

____ Street noises	____ Factory machinery
____ Crockery	____ Animal noises
____ Voices	____ Clear
____ PA System	____ Static
____ Music	____ Local
____ House noises	____ Long distance
____ Motor	____ Booth
____ Office machinery	Other _____

THREAT LANGUAGE:

____ Well spoken (educated)	____ Incoherent
____ Foul	____ Taped
____ Irrational	____ Message read by threat maker

REMARKS: _____

Report call immediately to:

_____ .

Phone number _____ .

Date __/__/__ .

Name _____ .

Position _____ .

Phone number _____ .

Figure 2-1. Sample Bomb Threat Checklist.

CHECKLIST

INSTRUCTIONS: BE CALM. BE COURTEOUS. LISTEN, DO NOT INTERRUPT THE CALLER. NOTIFY SUPERVISOR/SECURITY OFFICER BY PREARRANGED SIGNAL WHILE CALLER IS ON LINE.

Date_____ Time_____

Exact Words of Person Placing Call: _____

_____

_____

QUESTIONS TO ASK:

1. When is the bomb going to explode? _____
2. Where is the bomb right now? _____
3. What kind of a bomb is it? _____
4. What does it look like? _____
5. Why did you place the bomb? _____

_____

TRY TO DETERMINE THE FOLLOWING (CIRCLE AS APPROPRIATE)

Caller's Identity: Male Female Adult Juvenile Age _____ years

Voice: Loud Soft High Pitch Deep Raspy Pleasant Intoxicated Other _____

Accent: Local Not Local Foreign Region

Speech: Fast Slow Distinct Distorted Stutter Nasal Slurred Lisp

Language: Excellent Good Fair Poor Foul Other

Manner: Calm Angry Rational Irrational Coherent Incoherent Deliberate Emotional Righteous Laughing Intoxicated

Background Noises: Office Machines Factory Machines Bedlam Trains Animals Music Quiet Voices Mixed Airplanes Street Traffic Party Atmosphere

ADDITIONAL INFORMATION: _____

_____

_____

_____

ACTION TO TAKE IMMEDIATELY AFTER CALL: Notify your supervisorsecurity officer as instructed. Talk only to persons designated by your supervisor security officer.

_____

RECEIVING TELEPHONE NUMBER **PERSON RECEIVING CALL**

Figure 2-2. Checklist.

Fire Department. Fire is common when there is an explosive detonation. Early notification of the fire department can help minimize property damage and injury if the bomb should detonate. Fire department personnel will normally respond to the scene and stand by.

Medical Personnel. The potential for injury with a bomb threat is high. Trained personnel standing by is very important. Medical personnel should stand by the scene of a bomb threat with an ambulance.

Emergency Operations Center. It is necessary during any bomb situation to have a bomb threat emergency operations center (EOC) located at the bomb site. The EOC serves as a control point for search teams, communication, access lists, and release of information. This eliminates confusion as to who is in charge.

The post commander designates a bomb scene officer, and an alternate, to be in charge of the bomb site operation. The bomb scene officer and his alternate must have special training in bomb threats and emergency situations. Either the bomb scene officer or his alternate will respond to all bomb threats as the commander's representative.

The only person who may authorize release of information from the bomb site is the bomb scene officer. The only person who should release the information to the public is the public affairs officer (PAO). Keeping a tight control of information could prevent a wave of bomb threats.

Reliable communications from the bomb scene is essential. Radio transmissions will not be used within 150 feet (50 meters) from the suspect area. Note that some SOP may state 100 meters as the safe distance. Radio transmissions could detonate the bomb prematurely. All elements should attempt to maintain communication by telephone if possible.

Other methods that may be necessary include:

- Runners.
- Whistles.
- Field phones - TA 312.
- Hand signals (if one point is visible by all).

A CID Action Record (CID Form 66) will be initiated whenever a bomb threat is reported to a USACIDC unit.

A criminal investigation will be initiated on bomb threat incidents when a bomb is located or detonated, a subject is identified, or a series of related threats occur. In all other bomb threat incidents, a Serious Incident Report (SIR) will be prepared and the CID Form 66 will be completed.

Part D: DISCUSS EVALUATION AND EVACUATION CONSIDERATIONS

1. Evaluation Considerations.

Evaluation of the bomb threat is carried out by the bomb scene officer. He considers the results of the bomb threat checklist, information from support agencies, and the mission of the targeted facility. With this in mind, he must decide which of the three following actions to take.

- o Business as usual.
- o Search without evacuation.
- o Evacuation.

2. Business as Usual. After evaluating all the evidence at hand, the bomb scene officer may feel that the credibility of the caller is questionable. He may decide to go about business as usual. This might be the case if the caller is recognizable from previous hoaxes. The bomb scene officer will still report the message to other authorities. This action should be taken only when the likelihood of hoax is extremely great and there will be interruption of operations if any search is made.

3. Search Without Evacuation. A hoax may be suspected, but it is not obvious. The bomb scene officer can elect to conduct a search without evacuation. This search may be overt or covert depending on the facility and the likelihood of interrupting operations.

4. Evacuation. If the bomb threat was a descriptive one, the possibility of an actual bomb being present is greatly increased. In this case, evacuation is called for. The bomb scene officer should consider that personnel evacuation might expose them to greater danger. Also, the bomb scene officer must consider the time the bomb is set to go off, if the caller reveals this information.

The following is a list of considerations involved in evaluating a bomb threat:

- o An evaluation of the person making the threat, his apparent motivation and demeanor.
- o When and where the bomb will go off.
- o Type of structure and how prone it is to damage.
- o Identification of a recurring threat.
- o Call caused by news reports of other calls.
- o Whether employees are excused from work when such threats are received.

Evacuation Consideration. As discussed, evacuation is determined only after a thorough evaluation by the bomb scene officer of all available information. He may decide to evacuate for a variety of reasons, such as a descriptive bomb threat. If a device is discovered, either as a result of a bomb threat or during routine operations, an evacuation should be carried out promptly.

Evacuation Procedures. Authority to evacuate rests with the bomb scene officer, commander, or supervisor of the building concerned. Re-entry to the building is decided by the bomb scene officer.

Have a signal for evacuation. Proceed according to a set evacuation plan.

Evacuation teams should guide the occupants out of the area. These teams should be designated before the incident and be highly trained.

Evacuation must occur with the same compliance and speed as that of a fire drill. Public areas are the most likely place for bombs to be placed. They are the usual routes for evacuation. If time permits, a thorough search of these areas should be done before evacuation. This includes areas outside the building.

Individual responsibilities differ from a fire drill in the following ways:

- All persons will make a preliminary search around their immediate areas for suspicious items.
- All persons, as they leave, will remove those items that they brought in (briefcases, thermos bottles, lunch bags), turn off radios and unplug office machines.
- Windows and doors will be left open to help dissipate any explosive force.
- All cabinets and drawers will be left unlocked (except classified cabinets) to make it easier for the searchers.
- When evacuation of a building is completed, the building must be secured to prevent re-entry by unauthorized personnel.

When a bomb is found, evacuation will differ. Routes will be determined that will evacuate those closest to the bomb first. This will also depend on the type of building. In buildings with more than one story, rooms on floors above the danger point and just below should be evacuated first. Also, on the same floor as the bomb, evacuate three rooms away on all sides.

All persons will evacuate to a predetermined assembly area. A total accounting of all personnel will be done in this assembly area. This will determine if anyone still remains in the building. Secondly, it gives access to people who can verify if objects found belong in their area or not.

Evacuation Distances. Occupants should be evacuated to an area at least 100 meters away from the threatened area. This distance takes into account the force of items like propane bottles, natural gas lines, or welding equipment that would contribute to the explosive force of a bomb within a facility. It should be emphasized that this is a minimal distance. Greater distances would provide added safety. In any case, evacuees should be instructed to take cover and shelter from possible fragmentation.

Methods of Evacuation. Depending on the mission of the facility, it may be necessary to use different methods of evacuation. A partial evacuation is one such method. Evacuation of adjacent areas first as described above is another. Some areas where partial evacuation may be necessary are:

- o Hospitals.
- o Special weapons areas.
- o Classified storage areas.

Partial evacuation will involve risks. There are no guarantees as to what damage will occur if a device should detonate. If a device is actually found, total evacuation is more desirable than partial evacuation.

Part E: DISCUSS SEARCH PROCEDURES

The search for explosive devices is one of the most important actions involved in the bomb-threat procedures.

1. Search Personnel.

Except for the most unusual circumstances, EOD and Military Police will NOT be used to search for reported bombs in barracks, community areas, buildings, and offices. Such searches will be conducted by designated persons familiar with the area and its contents. Also, occupants will search their own work areas with designated search teams.

2. Supervisor Search.

Buildings must be inspected on a regular basis. This will reduce the possibility of an explosive or incendiary device being placed. It will also minimize the time required for the search after a threat has been received. Periodic inspections will reveal hiding places for bombs, possible targets, and building weaknesses. The inspector will become so familiar with his area that he should notice any new or strange item at once. The inspector should be the supervisor in his area or a member of a predesignated search team.

3. Search Teams.

There are three groups of persons who may be considered to serve as members of the search team. They are building supervisors, building occupants, and special search teams. Of the three, the specially trained search teams are

the most effective. This is especially so when combined with a brief search by occupants before they are evacuated.

4. Search Procedures.

A bomb threat usually brings to mind a picture of a bomb hidden inside a facility, but devices may be planted against a facility. A great amount of damage can be caused by a device planted outside a facility. Therefore, the search must proceed from the outside to the inside, and from the bottom to the top. These procedures have resulted from years of practical experience. This reduces the risk of injury to both the searchers and the occupants. It is preferable to search all areas at the same time if the search team is large enough. The following breakdown of team members has been found to be effective:

- Outside search - 25 percent.
- Inside search - 50 percent.
- Public areas - 25 percent.

Of course, if the location of the bomb is known or suspected, the search should begin in that area.

a. Exterior Search. The search of the outside of a building is more important. This is the most accessible area to the bomber, especially after dark. It must cover all feasible areas where a device may have been planted. The search pattern begins at ground level. Close attention must be given to the following:

- Window ledges.
- Bushes.
- Piles of leaves or refuse.
- Entrances.
- Garbage cans.
- Manholes.
- Flower arrangements.
- Air conditioner units.
- Automobiles (extreme caution must be used when the search involves automobiles).

The search should be conducted to a distance of 25 to 50 feet from the building (see Figures 2-3, 2-4, 2-5, 2-6). After completing the ground-level

search, return to the building and search window ledges, air conditioning units, signs, building ornamentation, fire escapes, and the roof. After completing the outside search, the outside search team may then be added to the inside search teams.

b. Internal Search. Except in cases of simultaneous searches, the inside search begins after the outside search. Search of the inside will begin with the basement.

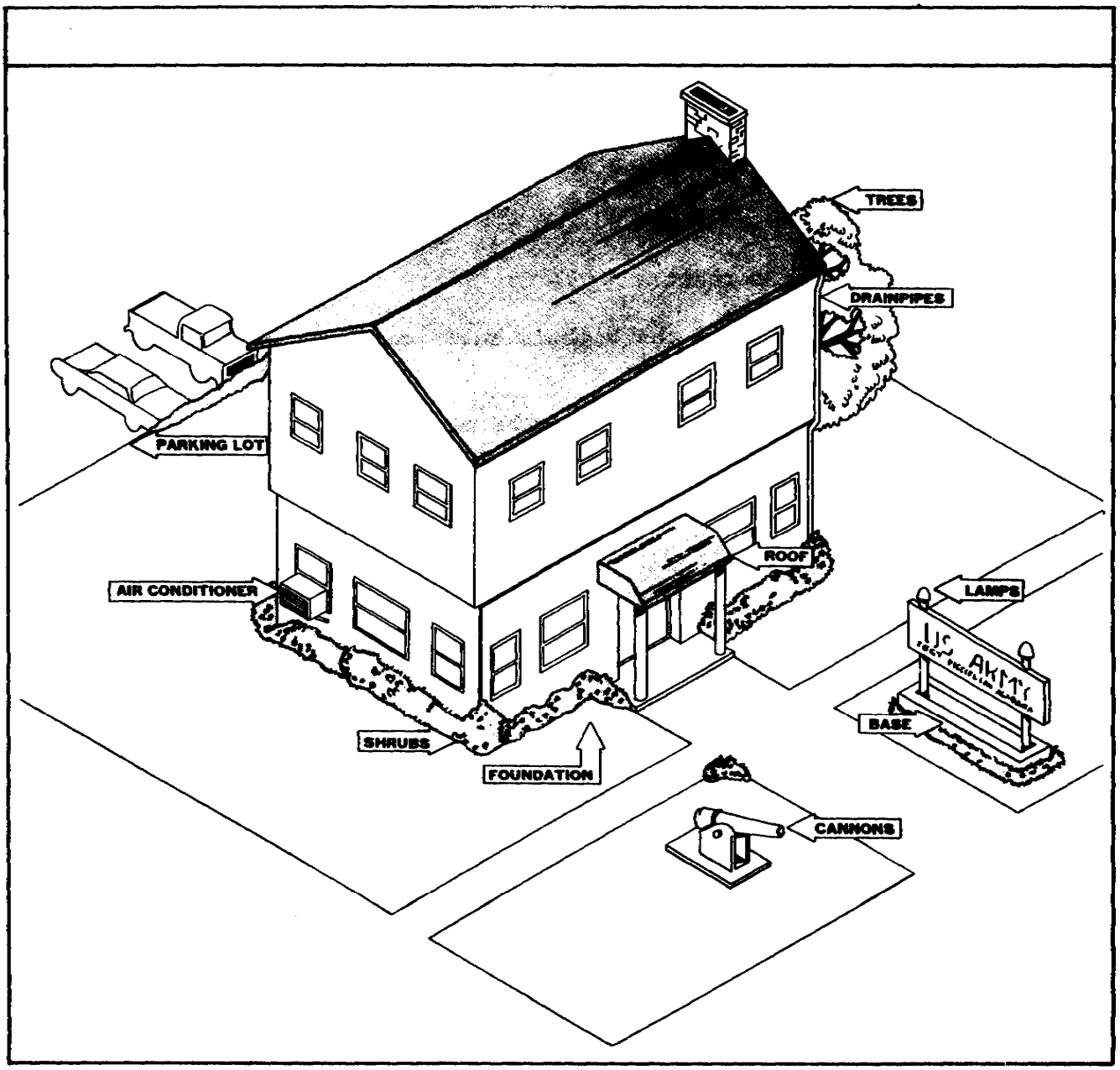


Figure 2-3. Search Areas.

Work toward the top floor, and from public access areas to more restricted access areas. If a separate public-area team is set up, use building custodial personnel or others familiar with the areas. Rooms that have been searched should be marked with crepe paper or tape. This will prevent duplication in the search.

Upon entering a room, searchers should remain still with eyes closed and listen. Often, clockwork timing devices can be detected without special equipment. Next, take a quick visual scan for any obvious unusual items. Divide the room in equal parts according to the number of objects to be searched, not by the size of the room (see Figure 2-7).

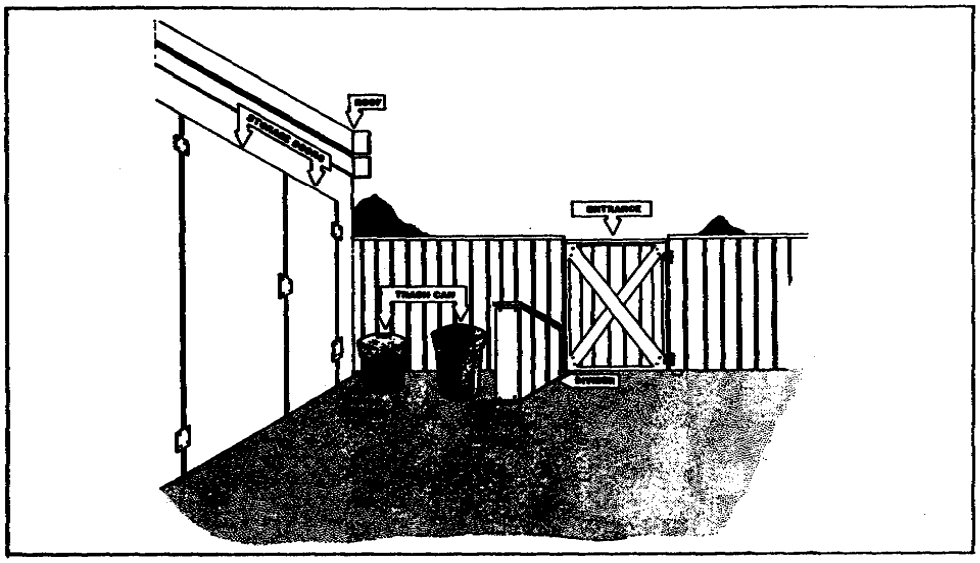


Figure 2-4. Search Areas.

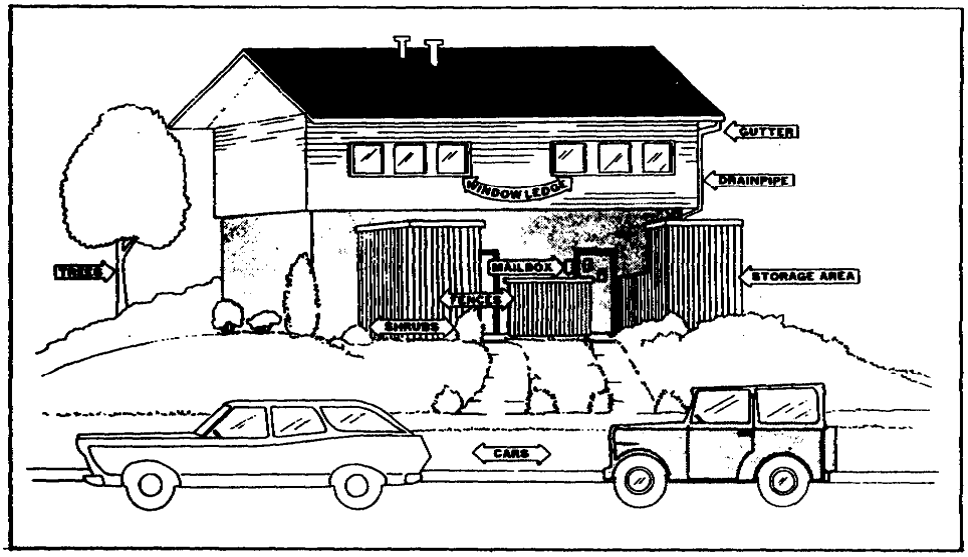


Figure 2-5. Search Areas.

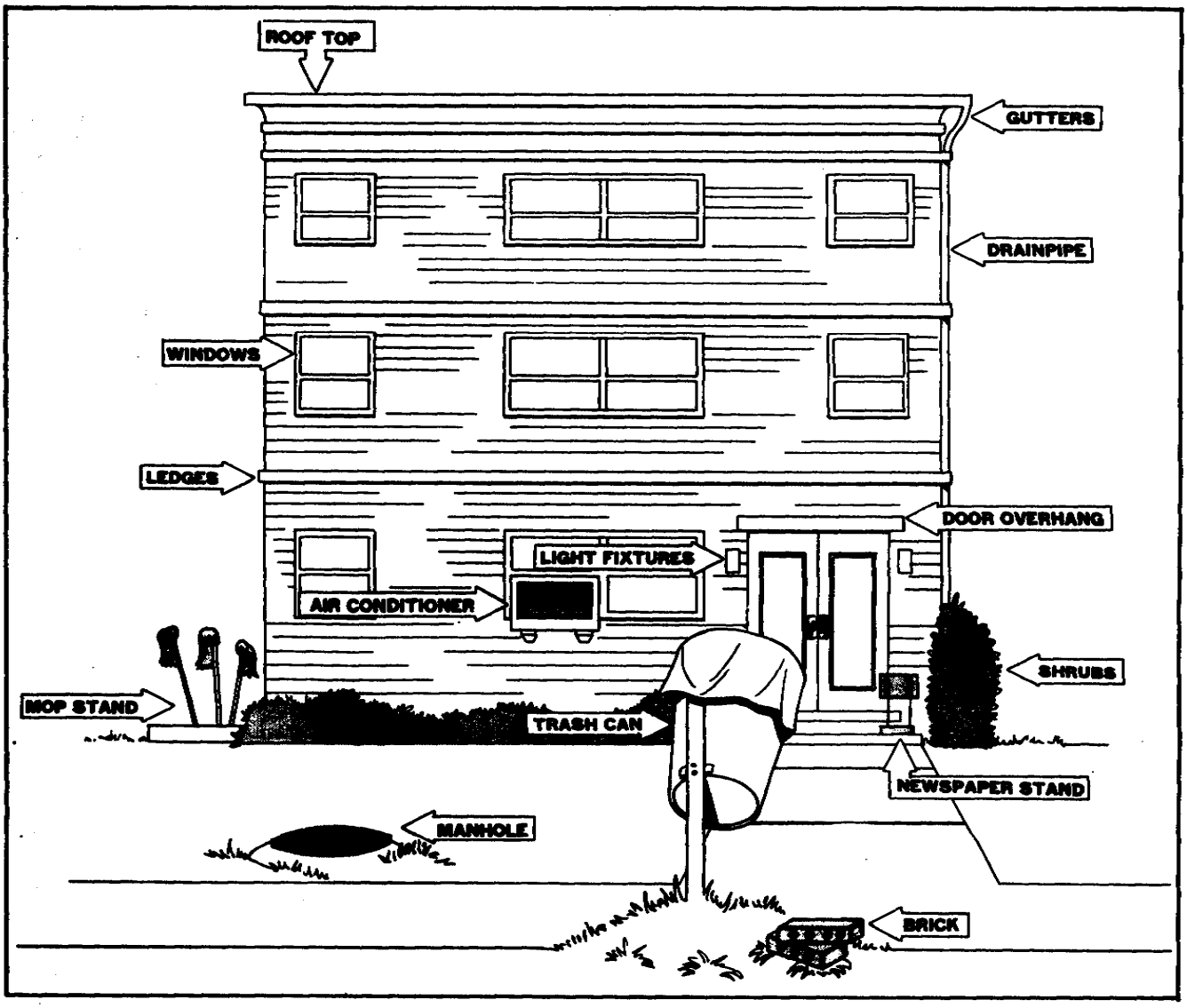


Figure 2-6. Search Areas.

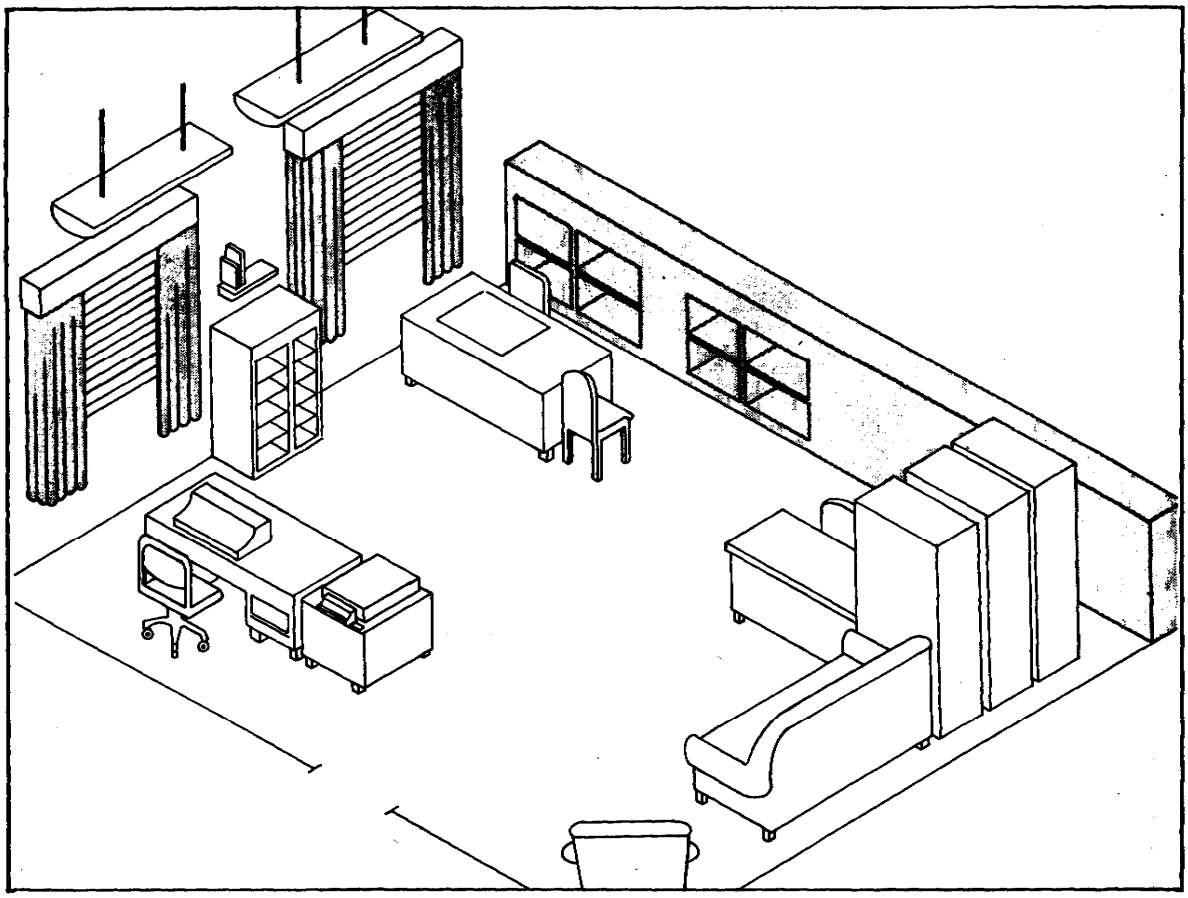


Figure 2-7. Divide Officer Area Before Searching.

Next, divide the room into four levels. The first sweep of the room will include all objects from the floor to waist level. This sweep will take the most time and effort because it includes almost all items of furniture and underneath rugs (see Figure 2-8).

The second level of search includes everything from the waist to the chin. This will include items such as table tops, filing cabinets and lower shelves.

The third level of search includes all items from the chin to ceiling. This will include picture frames, shelves, cupboards, windows, and vents.

The last level includes anything above the ceiling if it is false. Check vents, pipes, indirect lighting fixtures and ceiling supports.

It may be necessary in larger rooms to use two or more teams to conduct a thorough search. Figure 2-9 shows one approach to this situation.

The room search is ended only when the person in charge is satisfied that an adequate search has been made. A searcher should never say, "There is no bomb." He should say only, "No bomb was found."

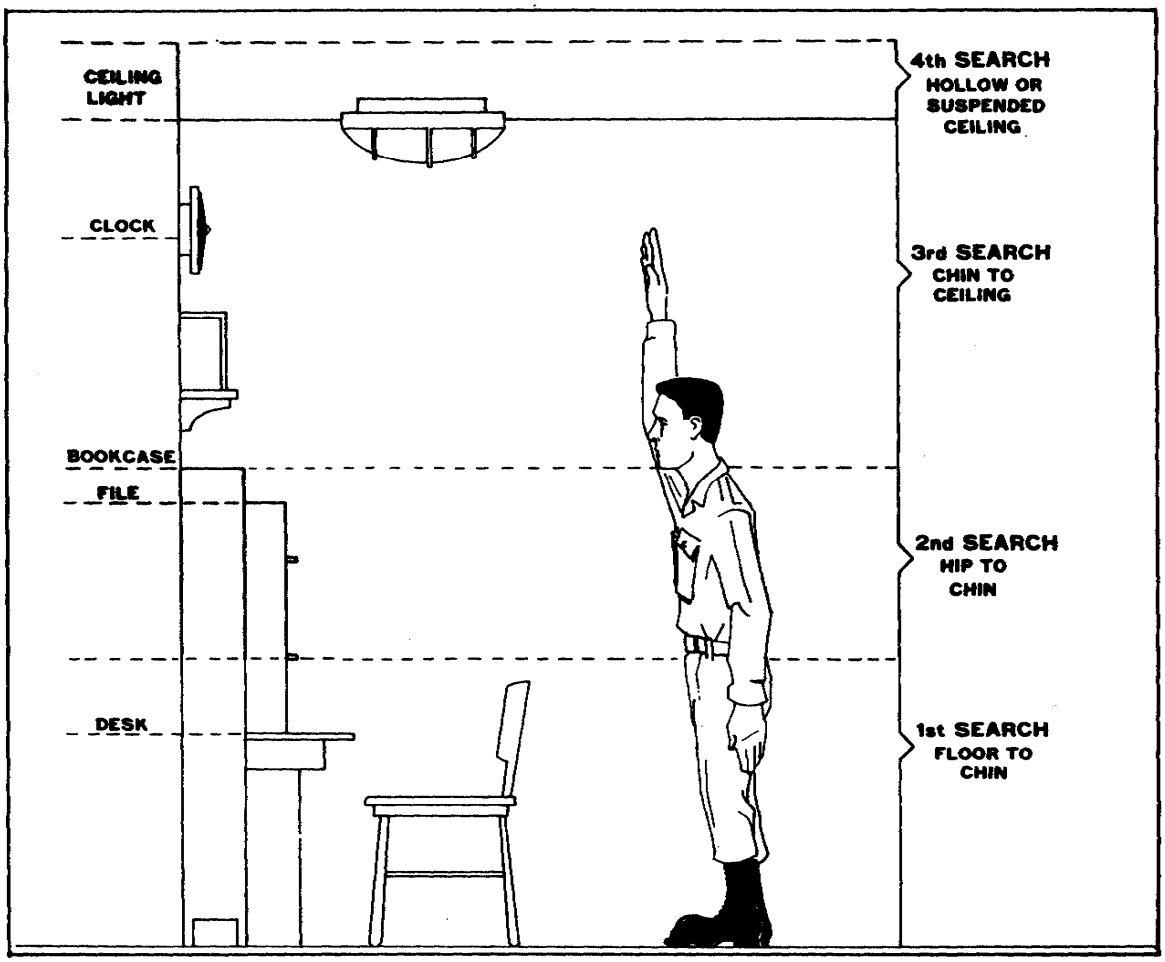


Figure 2-8. Search Areas.

5. Equipment.

The following equipment can be life saving to search teams:

- o Common tool set consisting of pliers, crescent wrench, and both phillips and straight screwdrivers. These tools should only be used to gain access to areas to which the bomber may have access.
- o A flashlight, preferably with a light bending adaptor to allow searchers to look into small openings.
- o Hand mirror to use in conjunction with the flashlight to observe under and behind items.
- o Body armor, such as flak vest.
- o Plastic ribbon, string, or crepe paper for marking searched areas.

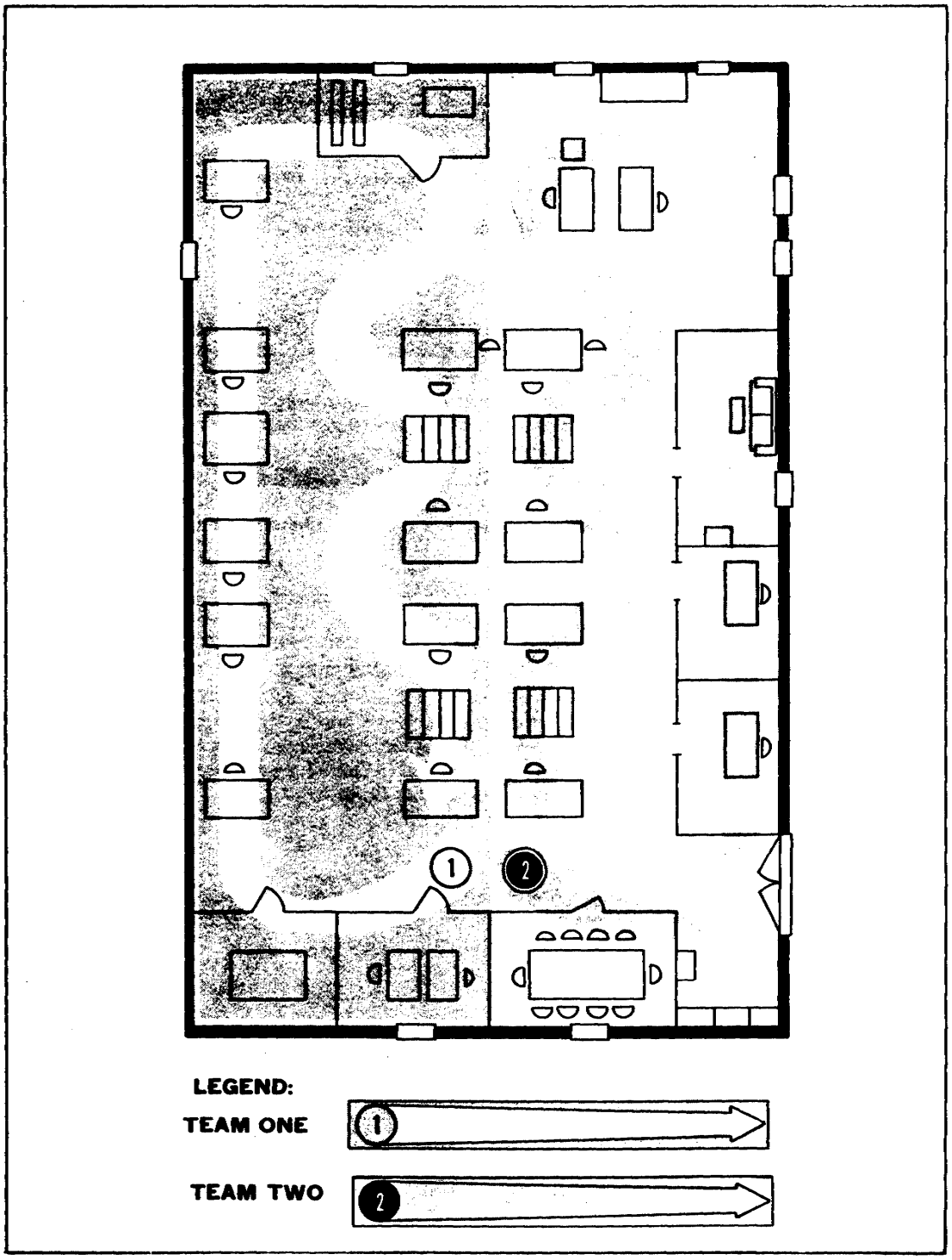


Figure 2-9. Search Patterns.

What to Search For

The search of even a medium sized building can take 12 to 24 hours. It is essential that the searchers be highly trained and know what to search for. EOD personnel offer two courses of instruction to requesting organizations. They are.

- Improvised Explosive Device Search Course.
- Explosive Ordinance Reconnaissance Course.

Since search teams are composed of persons familiar with the area to be searched, the main thrust of their search is for objects that do not belong in the area. Good housekeeping will aid in this task. Of course, objects that are familiar may be found to contain bombs upon close inspection. In this regard, training from EOD personnel may prove invaluable.

NEVER TOUCH A SUSPICIOUS OBJECT UNDER ANY CIRCUMSTANCES

The bomb scene officer may wish to keep a Search Checklist as shown in Figure 2-10.

If a bomb is found, the search should not be terminated as other bombs may also have been placed.

Part F: DISPOSAL PROCEDURES

If a searcher finds or suspects he has found a bomb, he should not touch the device. Instead, he should immediately clear the area and notify the emergency operations center (EOC). The EOC will then notify the EOD, who has responsibility to deactivate and remove the bomb.

1. Evacuation After Discovery.

If evacuation is not already completed, promptly evacuate all nonessential personnel. If they have already been evacuated, they should be moved further away, preferably behind a windowless structure.

2. Procedures for Minimizing Damage.

If EOD determines that time allows, attempt the following:

- Disconnect or shut off any gas lines leading to the facility.
- Open windows and doors.
- Remove items which may add to the explosive force (gasoline, lubricants, paints, etc.)

Yes	No	
____	____	Were all areas assigned to some member of the search team?
____	____	Was the outside of the building and surrounding area searched?
____	____	Were the assignments to areas based on knowledge of the area?
____	____	Was key control established; were all doors unlocked?
____	____	Did search-team members know their area assignments?
____	____	Did search-team members know their responsibilities when a bomb or suspected bomb was found?
____	____	Were communication procedures established?
____	____	Were proper search techniques followed?
____	____	Was there an audio check?
____	____	Were rooms divided by area?
____	____	Were rooms divided by height?

What actions were taken when a "bomb" was found? _____

_____

_____

What search techniques were used? _____

_____

_____

What method(s) of communication was used? _____

_____

_____

What areas were not searched? _____

_____

_____

Figure 2-10. Search Checklist.

- o Sandbag the area around the device, but never place any item on the device itself.

If a bomb should explode, damage control teams, first aid teams, heavy and light rescue teams, and communication teams should be on hand. Damage control teams will go to the scene of the explosion and attempt to control any fires; remove flammable items; allow venting; disconnect utilities, as applicable; and have fire and medical teams stand by. Rescue teams will go to the scene to assist and evacuate any injured parties. First aid teams will report to the established aid station. They will administer first aid to the injured. Communication teams will establish communications between these first aid teams and the control center. All of these teams should remain outside the 100 meter evacuation radius until they are needed.

In the case of an actual bombing, all personnel are warned not to tamper with debris. Procedures for searching the detonation site for physical evidence should be followed as for any crime scene.

The post public affairs officer is the only person who should release information to the press. All other personnel should be instructed not to discuss the current situation with anyone. This ensures accurate information will be given to the news media. More importantly, it will minimize future bomb-threats.

LESSON 2

PRACTICE EXERCISE

This practice exercise is designed to test your knowledge of the material. This lesson covered bomb threat contingency planning. To check your comprehension of the lesson, complete the practice exercise below. All of the questions are multiple-choice with one correct (or best) answer. Try to answer all the questions without referring to the lesson material.

When you have answered all of the questions, turn the page and check your answers against the answer key. Review any questions you missed or don't understand. When you have completed your review, continue to the next lesson.

1. In preparing security against would-be bombers, it is necessary to be aware that most bomb designs are based on what?

A. Extremist publications.
B. United States Army publications.
C. Libyan terrorist manuals.
D. Commercially published books.

2. Based on your knowledge of the primary bombing targets of bombers, your preplanning would include which of the following?

A. Isolating important military personnel.
B. Daily searches in classified areas.
C. Increasing security at residences.
D. Focusing on military installations.

3. As a mail room worker, you receive a suspicious package. What would you do?

A. Open it immediately.
B. Not open it, but place it in water immediately.
C. Return it to the sender.
D. Isolate the package and evacuate the area.

4. In defending against bomb threats, security efforts will be made with the understanding that anti-establishment sentiment is what?

A. A secondary reason for bombings.
B. A non-political motive.
C. The number one reason for residence bombings.
D. A psychological disorder.

5. You have received a telephone bomb threat. In your conversation with the caller, what should you do?

A. Ask him to complete a CID Form 66.
B. Be prepared to paraphrase his threat.
C. Not allow any other individuals to listen in.
D. Ask his name and location.

6. As a bomb scene officer, you should be aware that bomb threat notification will result in what?

A. Military Police arriving and conducting a search of the facility.
B. EOD not responding unless a suspicious item is located.
C. Fire department personnel standing by, responding to the scene if the bomb should detonate.
D. All suspicious items being opened upon discovery.

7. As Military Police commander, how should you consider bomb threat; evidence?

A. Important to the bomb scene officer's evaluation.
B. Make an evaluation of the situation.
C. Releasable to the news media.
D. Outside the jurisdiction of the USACIDC.

8. Your room or office is being evacuated because of a bomb threat. What should you do?

A. Conduct yourself with the same compliance and speed as a fire drill.
B. Leave the windows and doors open, and leave your personal items in the room.
C. Touch nothing and leave the room as it is.
D. Close the windows and doors, and remove all personal items.

9. In searching a facility after a bomb threat has been received, the bomb scene officer will NOT have what?

A. Occupants involved because they are not trained searchers.
B. EOD search because they enter the area only after a bomb is found.
C. Military Police available because they will not be in the area.
D. Search teams of less than six men.

10. A bomb is suspected of being placed at a troop billet. As a search team member your search should proceed how?

A. From the inside to the outside, top to bottom.
B. From the outside to the inside, bottom to top.
C. From the outside to the inside, top to bottom.
D. From the inside to the outside, bottom to top.

11. Your search team has discovered an obvious bomb. What would you do?

A. Not touch it and report to the bomb scene officer.
B. Place the bomb in water until EOD arrives.
C. Attempt to deactivate it.
D. Not touch it and wait for Military Police to do so.

12. Despite your best efforts, a bomb explodes before it can be found and deactivated. What would you do as the bomb scene officer?

A. Instruct personnel to clear debris immediately.
B. Release all available information to the news media.
C. Have damage control teams on the scene to control fires.
D. Place sandbags around the site.

LESSON 2

PRACTICE EXERCISE

ANSWER KEY AND FEEDBACK

Item		Correct Answer and Feedback
1.	B.	United States Army Publications. United States Army . . . (page 2-2, para 1).
2.	C.	Increasing securities at residence. According to the National Bomb . . . (page 2-5, para 1).
3.	D.	Isolate the package and evacuate the area. Instead they should . . . (page 2-4, para 2).
4.	A.	A secondary reason for bombings. Despite the growth of . . . (page 2-6, para 3).
5.	D.	Ask his name and location. The receiver should attempt. . . (page 2-7, para 1).
6.	B.	EOD not responding unless a suspicious item is located. Normally, EOD personnel will NOT . . . (page 2-8, para 2).
7.	A.	Important to the bomb scene officer's evaluation. Evaluation of the bomb . . . (page 2-12, para 1).
8.	A.	Conduct yourself with the same compliance and speed as a fire drill. Evacuation must occur with. . . (page 2-13, para 4).
9.	B.	EOD search because they enter the area only after a bomb is found. EOD personnel will NOT . . . (page 2-8, para 2).
10.	B.	From the outside to the inside, bottom to top. Therefore, the search must proceed. . . (page 2-15, para 4).
11.	A.	Not touch it and report it to the bomb scene officer. If a searcher finds or suspects. . . (page 2-22, Part F).
12.	C.	Have damage control teams on the scene to control fires. Damage control teams will. . . (page 2-24, para 2).

LESSON 3

COMBATTING TERRORISM

Critical Task: 01-3755-00-5000

OVERVIEW

LESSON DESCRIPTION:

In this lesson you will learn to recognize terrorism and utilize a crisis management team.

TERMINAL LEARNING OBJECTIVE:

ACTION: Describe the basic principles of terrorism. Describe crisis management team composition, capabilities, and responsibilities for contingency planning.

CONDITIONS: You have this subcourse, paper and pencil.

STANDARDS: To demonstrate your competency of this task you must achieve a score of 70 percent on the subcourse examination.

REFERENCES: The material contained in this lesson was derived from the following publications: AR 190-13, AR 525-13, FM 19-10, FM 19-15, FM 100-37, and CIDR 195-1.

INTRODUCTION

Recent increases in the number of terrorist acts and hostage situations make it essential that the Military Police (MP) are prepared to provide protection from, and control of, these types of situations. These acts are often performed in desperation or because of fanaticism. It is essential that all MP understand their role and perform their duties as well as possible. Dealing with these situations in an efficient, direct manner reduces the chance of personnel being injured or killed, and of property being damaged or destroyed.

PART A: THE DEFINITION AND HISTORICAL OVERVIEW OF TERRORISM

The following three selected definitions of terrorism reflect the varying ways in which terrorism is perceived. However, there are some common threads in the definitions.

Terrorism. The calculated use of violence or the threat of violence to attain goals, often political, religious, or ideological in nature, through fear, intimidation or coercion. It involves a criminal act often symbolic in nature and intended to influence an audience beyond the immediate victim, AR 525-13.

Terrorism. Violence for effect. . . not primarily, and sometimes not at all for the physical effect on the actual target, but rather for its dramatic impact on an audience. . . .Brian Jenkins, Rand Corporation. Terrorism. Violent, criminal behavior designed primarily to generate fear in the community, or a substantial segment of it for political purposes. Disorders and Terrorism, National Advisory Committee on Criminal Justice standards and Goals, LEAA.

Terrorism stripped to its basic elements is:

- o A criminal act.
- o The systematic use of violence for effect.
- o Aimed at the audience watching.

Terrorists consider military and police forces their opponents. The military and the police are seen as the protectors of society. Terrorists believe that successful attacks on security force targets expose the weaknesses of a society. They believe successful acts also help show how effective terror is as an agent of change.

1. Understanding the Historical Overview of Terrorism.

This course is not designed to examine the complete history of terrorism. However, some brief examples of previous terrorist activity will be given for background purposes.

2. Historical Overview.

History is filled with examples of persons, groups, and often national leaders, who have used terror tactics for one reason or another. Robespierre used terror tactics to destroy the French aristocracy in the 18th century, when an estimated 40,000 people were executed. The Russian Socialist Revolutionists attempted to use terror tactics to overthrow the Czar in the beginning of this century, only to be thwarted by the Bolsheviks who combined the strategy of mass with tactics of terror to succeed where pure terrorism had failed. The majority of pre-modern terrorism has been motivated by the desire to be free from colonialism. Contemporary terrorism, however, has taken on new elements that make it more complex.

3. Modern Terrorism.

Some commentators on terrorism appear to agree that the roots of present terrorism lie in the swell of student unrest during the 1960's. That is when there was a general global trend towards dissatisfaction with the establishment. Others claim terrorism is merely the violent reaction of the

Third World to the long exploitation and manipulation of resources and technology by the more affluent nations, such as the United States. Whatever the cause, the use of violence to make a point became more popular. The problem will continue to plague modern society. Modern terrorism has elements which differ from older forms of violence. This makes terrorism in today's world a greater threat than ever before.

4. The Media.

No matter what the terrorists' cause may be, one of their main objectives must be to publicize their cause to the widest audience possible. The existence of a highly efficient media network, therefore, is a factor in any terrorist scenario. This must not be underestimated. Today's technology gives terrorists the opportunity to gain world attention on prime time television on the same day, if not at the same time as the event. They are guaranteed column inches and banner headlines in the world press the following day. Indeed, there is seldom a day when terrorist's activities do not appear in national newspapers around the world.

Beyond this basic premise, there are some inherent problems when the media cover terrorist activity. In an endeavor to get the best story, reporters sometimes glamorize the events to make the story worthwhile. This helps the terrorists to publicize their causes. Moreover, it glorifies the very people who oppose the establishment. The additional and complementary danger is that the next terrorist acts are made deliberately more violent and horrific in order to gain increased publicity.

Communications.· The second factor to influence the new terrorism is communications. Technological advances in the last 15 years or so have enhanced the terrorist's capabilities for operating in any part of the world quickly, efficiently and with relative ease. This single factor has contributed to the growth of transnational and international terrorism in the last decade. It has also removed the terrorist from the realm of parochial freedom fighters.

The Potential for Superviolence. Here again technological advances may be seen to affect present day terrorists and their capabilities. The ability of terrorists is now greatly enhanced with the advent of surface-to-air and surface-to-surface missiles, of laser devices, and of chemical and nuclear weapons. In the wrong hands, today's technology could prove to be devastating. The problems posed to security agencies become unthinkable. Yet, we must learn to think of the unthinkable, for any scenario is possible. The only limitation lies in the imagination of the terrorists themselves.

Part B: DESCRIBE THE TERRORIST PROFILE

The Institute of Study of Conflict, when discussing terrorism, classified terrorist groups in the following ideological categories:

1. Minority Nationalist Groups. These groups are fighting the majority of the community. There, the support base will depend on the sympathy of ethnic, religious, or linguistic minorities at odds with the majority community. Examples are the Basque ETA, or the Black Liberation Army in the United States.

2. Marxist Revolutionary Groups. Here the terrorist movement has a coherent Marxist ideology (of any persuasion) and a long term strategy for bringing about a socialist revolution. The official wing of the IRA and the Italian Red Brigades are excellent examples.

3. Anarchist Groups. True anarchists are difficult to find. True anarchy brings lawlessness and disorder. This is not a natural state for the human race. Those purporting to be anarchists include the Moviemiento Iberio Libertario (MIL) in Spain, the Angry Brigade in UK, and Red Army Faction in Germany.

4. Pathological Groups. The Symbionese Liberation Army and the Weather Underground organizations are both grouped here by the Institute. The Institute also observed that pathological violence appears to be a phenomenon of persons such as Charles Manson, the Son of Sam, and the Hillside Strangler, rather than groups. Motivation normally has more to do with personal inadequacy, hatred of family, or specifically white middle-class guilt-feeling, than with acquired ideology.

5. Neo-fascist and extreme right-wing groups. The threat from right wing groups is steadily rising in Europe, in particular. Neo Nazis and Neo fascists groups are appearing to counter the activities of the left. They may pose just as serious a threat to security agencies as do the more traditional terrorist groups.

6. Ideological Mercenaries. Western Societies are now experiencing a new form of terrorism. Men and women, for the sake of a shared ideology and a common faith in worldwide revolution (rather than money), are ready to cross frontiers to pursue their cause. The Japanese Red Army (Rengo Sekigun) is cited as an example by the Institute. Another example is Carlos, The Jackal.

Terrorist groups are categorized by government affiliation to help security planners anticipate terrorist targets and their sophistication of intelligence and weaponry. Three general categories that have gained acceptance are--

- Nonstate supported. A terrorist group that operates autonomously, receiving no significant support from any government (for example, Italy's Red Brigades, Basque ETA).

- State supported. A terrorist group that generally operates independently, but receives support from one or more governments (for example, PFLP in the Middle East).

- State directed. A terrorist group that operates as an agent of a government receiving substantial intelligence, logistics, and operational support (for example, Libyan "hit teams").

The common strategy of the terrorist is to commit acts of violence which will draw the attention of the world to the cause. The victim is seldom his target. By threatening or carrying out acts of extreme violence against a victim, the terrorist is attempting to produce fear in the victim and the target; both of which are dependent upon the government for protection.

At the same time, the terrorist makes demands upon the government, which in turn, must have some reaction to the terrorist, target, and victim. Figure 3-1 illustrates the relationship in a terrorist situation.

PART C: DESCRIBE COMMON TACTICS USED BY TERRORISTS

1. Bombing.

The tactic most common to terrorist groups is bombing. Of all terrorist incidents recorded over the last decade, a little over 50 percent were attributed to the terrorist bomb. The bomb is a popular weapon. It is cheap to produce, easy to make, has variable uses, and is difficult to detect and trace after the event. The increase in bombing activity and the increase in sophistication of devices used has caused the NATO Explosive Ordinance Disposal Standardization Committee (EOD) to classify all terrorist bombs as Improvised Explosive Devices (IEDs). This makes them distinct from all others. The term IED is now commonly used by many law enforcement agencies as well as military forces.

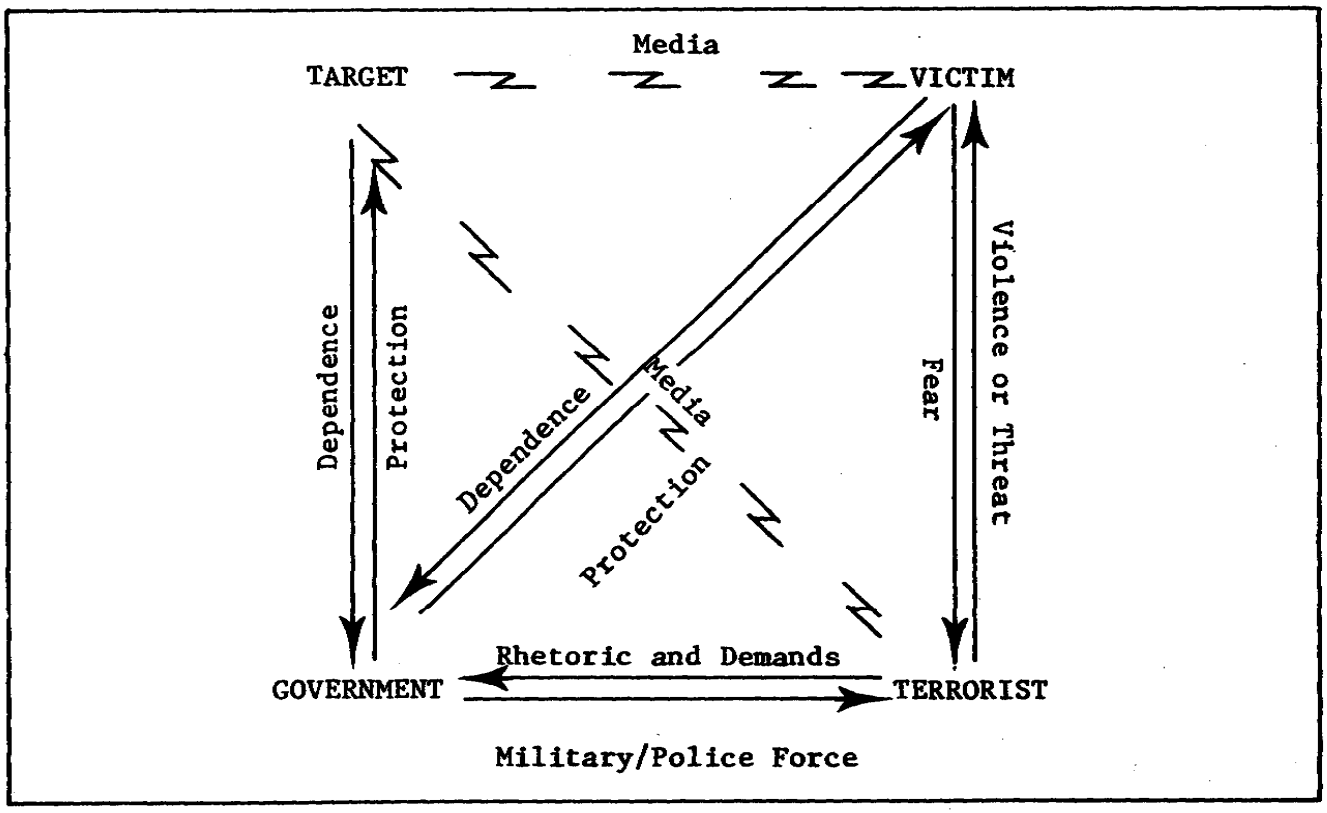


Figure 3-1. Relationship in Terrorist Situation

There are a number of ways to subclassify IEDs: by delivery means, by activation means, or by usage (see Figure 3-2).

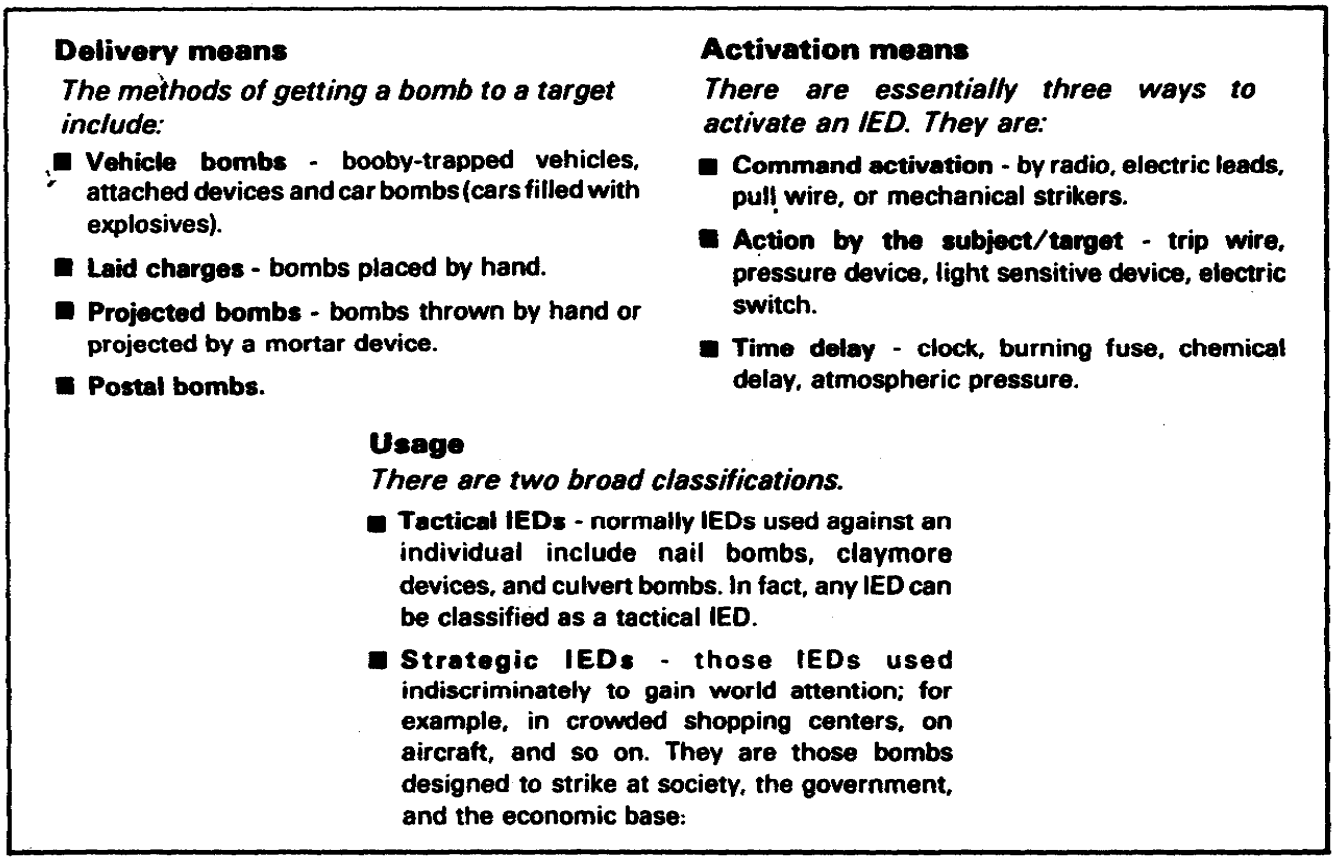


Figure 3-2. Subclassification.

2. Arson. Although not a tactic used by all terrorist groups, arson is a powerful weapon of destruction and disruption. Public utilities, commercial premises, and political buildings are frequent targets. A popular method of starting fires is by using time-delayed incendiary devices which are comparatively cheap and easy to make, easily concealed, and difficult to detect once planted.

3. Hijacking. Hijacking and skyjacking was very much an event of the 1960's and early 1970's. Hijacking of vehicles carrying staple foods was a favored tactic of the Tupemaros. It fitted their particular style of armed propaganda. The hijacking would be followed quickly by the free distribution of the vehicle's cargo to the poor and needy together with propaganda advertising the terrorist's cause. In any kind of continuing terrorist activity, such as in Spain or Northern Ireland, the hijacking of vehicles is associated with, and often gives indications of, some future atrocity. For example, the hijacking of a gasoline truck almost certainly indicates the future appearance of a 50,000 lb. benzine bomb (in the form of the truck wired with explosive). Additionally, hijacked "legitimate" vehicles give the terrorist an easy means to approach or gain entry to a closed military post.

4. Ambush. Well-planned ambushes seldom fail. This is especially true of terrorist ambushes which are generally well-thought out. Diversions and lay-off teams are often included in the plan that they rehearse and execute with precision. It is often forgotten that the terrorist has time on his side. He will spend weeks if not months preparing for the operation. To his advantage is the fact that the terrorist can choose his own time and place of operation. If his intended victim continually uses the same route, the terrorist can conduct countless rehearsals before the actual event.

5. Kidnapping. Not all ambushes are designed to kill the principal, as was proven in the Schlever and Moro ambushes and subsequent kidnappings. Both were acted out with extreme precision and with definite goals in mind by two separate, dedicated terrorist groups.

6. Hostage Taking. The difference between hostage taking and kidnapping is extremely fine in the world of terrorism; indeed the two terms are often interchanged. However, the kidnapper normally should be regarded as someone who confines his victim in a secret hideaway and makes material demands (money, weapons, etc.); whereas, the hostage taker will confront authorities and openly hold his victim for ransom. The hostage taker's demands are often more than just material in nature. Political concessions are often demanded in exchange for the lives of the hostages.

The importance of hostage taking as a fairly new and popular terrorist tactic is plain. First, because of its currency, hostage taking will attract the media. As one observer commented about the Iranian Embassy scene, "it is street theater." Second, the fact that live hostages are involved increases the drama of the event. Terrorists can then apply pressure to force concessions which otherwise might not be made. Finally, the hostage is a tangible asset to the terrorist. He finds he has something with which to bargain.

7. Assassination. Assassination is perhaps the oldest terrorist tactic. It is widely used today. Groups favoring the use of assassination include the Basque Separatists (ETA) in Spain, the Red Brigades in Italy, the Provisional IRA in Northern Ireland, Qdadafi's international terror groups, and more recently, both the FPL and FARN in El Salvador. Targets are often predictable, and invariably claimed after the event by the terrorists

themselves. All groups mentioned operate against government officials, corporate executives, and police and security officials.

Whatever else terrorist- tactics may be, they are certainly simple to apply, dynamic in their effects, and hit and run by nature. They are designed for their impact upon the public rather than the victim.

PART D: TYPICAL TERRORIST GROUP ORGANIZATION AND THE TERRORIST INTERNATIONAL NETWORK

Little detailed information is available about specific terrorist groups. The basic necessary ingredients for an organized terrorist group are represented in Figure 3-3.

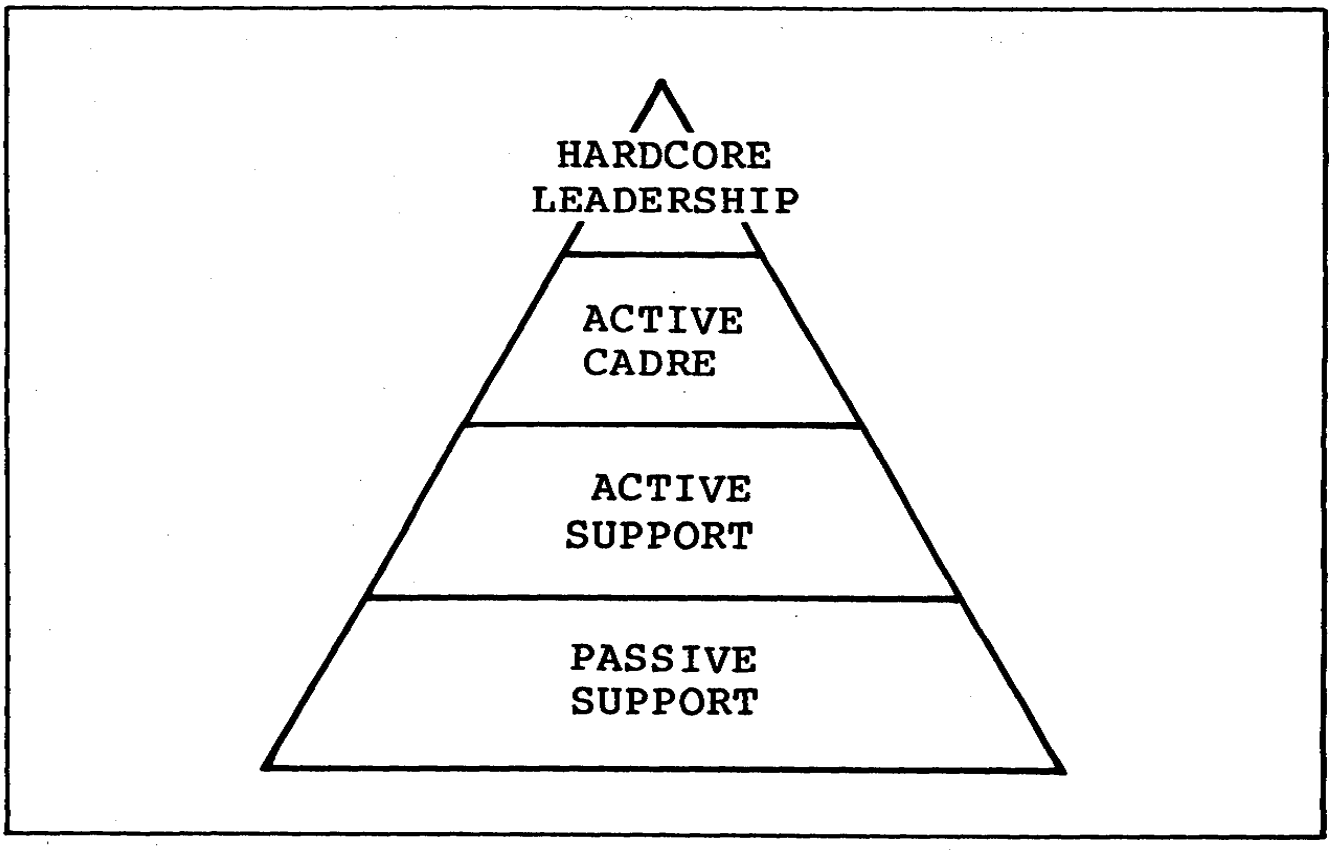


Figure 3-3. Organized Terrorist Group.

1. Leaders. With the exception of some anarchist groups, all terrorist groups boast a leadership in some form or another. As in military circles, leadership is necessary to make policy, lay plans, and give direction. In the terrorist world, leaders are often paranoid and fanatical. Yet, they may have

a legitimate front, behind which they operate consistently. In smaller organizations, the leadership may be the same as the active cadre.

2. The Active Cadre. The active cadre are the doers, the people of action who carry out the orders from their higher commands. They are normally organized into small active service units or cells. Each unit or cell will normally specialize. A typical cell may consist of 4 to 6 bombers, arsonists, assassins, and so on. With few active cadre, secrecy is easy to maintain. In most groups only one terrorist from one cell will know one other terrorist in another cell. The active cadre also will contain the trainers. Most of them maintain their skills through on the job training (OJT). These people are criminally violent and are willing to kill.

3. Active Supporters. The active supporters provide the support needed to sustain terrorist operations. They provide safe houses, weapons, ammunition, vehicles, medical support, food, money, the list seems endless. Active supporters often come from the professional classes, for example, lawyers, doctors, and businessmen. In summary, the active supporters normally provide a source of new blood to the active cadre. These persons are not willing to conduct violent criminal acts.

4. Passive Supporters. The passive supporters are the most difficult elements to define and recognize. They consist of those people sympathetic to the cause, but will not stand up and be counted through the fear of becoming involved. They also consist of those people who may be ignorant of the true aims of the cause and ignorant that their support is important to the politically motivated terrorist who needs overall popular support to survive. It is from this passive support that the popular support derives. Passive supporters often unwittingly provide donations in the form of cash. They are also relied upon heavily to "spread the word."

The diagrams in Figure 3-4 represent the cellular structure of terrorist organizations in both small (40-50) and moderately-sized (100-500) groups.

Although there is no apparent worldwide conspiracy, a trend toward cooperation has developed among terrorist groups. This includes sharing resources, expertise, and safe havens, and conducting joint operations. The list of benefits is considerable; arms, ammunition, money, intelligence, explosives, and safe houses. The Lod Airport massacre is a good example of this network in operation when members of the Japanese Red Army (JRA) returned a favor to the Popular Front for Liberation of Palestine (PFLP) on May 30, 1972. Their preparation and planning included traveling to the U.S., Canada, France, and then to Lebanon. There, they were instructed in guerrilla tactics at a Fedayeen training camp. They then traveled to Rome where they were supplied with Czech weapons and ammunition. They went on to a safe house in Rome where they waited to travel to Tel Aviv to commit the final acts.

5. Sovereign State Support.

Many terrorist groups also receive help from social, ethnic, and political groups in their area of operations. These countries and organizations provide

funds collected from people sympathetic to the causes. Many terrorists in Western Europe and the Middle East have been trained in the Soviet Union, North Korea, Algeria, Libya, and South Yemen. Japanese and Western European terrorists have received training in Lebanon, Viet Nam and South Yemen. In the Middle East, popular support for terrorism does exist. Large terrorist groups move in freedom and often conduct open meetings. These groups are very formidable due in part to the money, training, and arms support received from host countries such as Iran, Syria, and Libya.

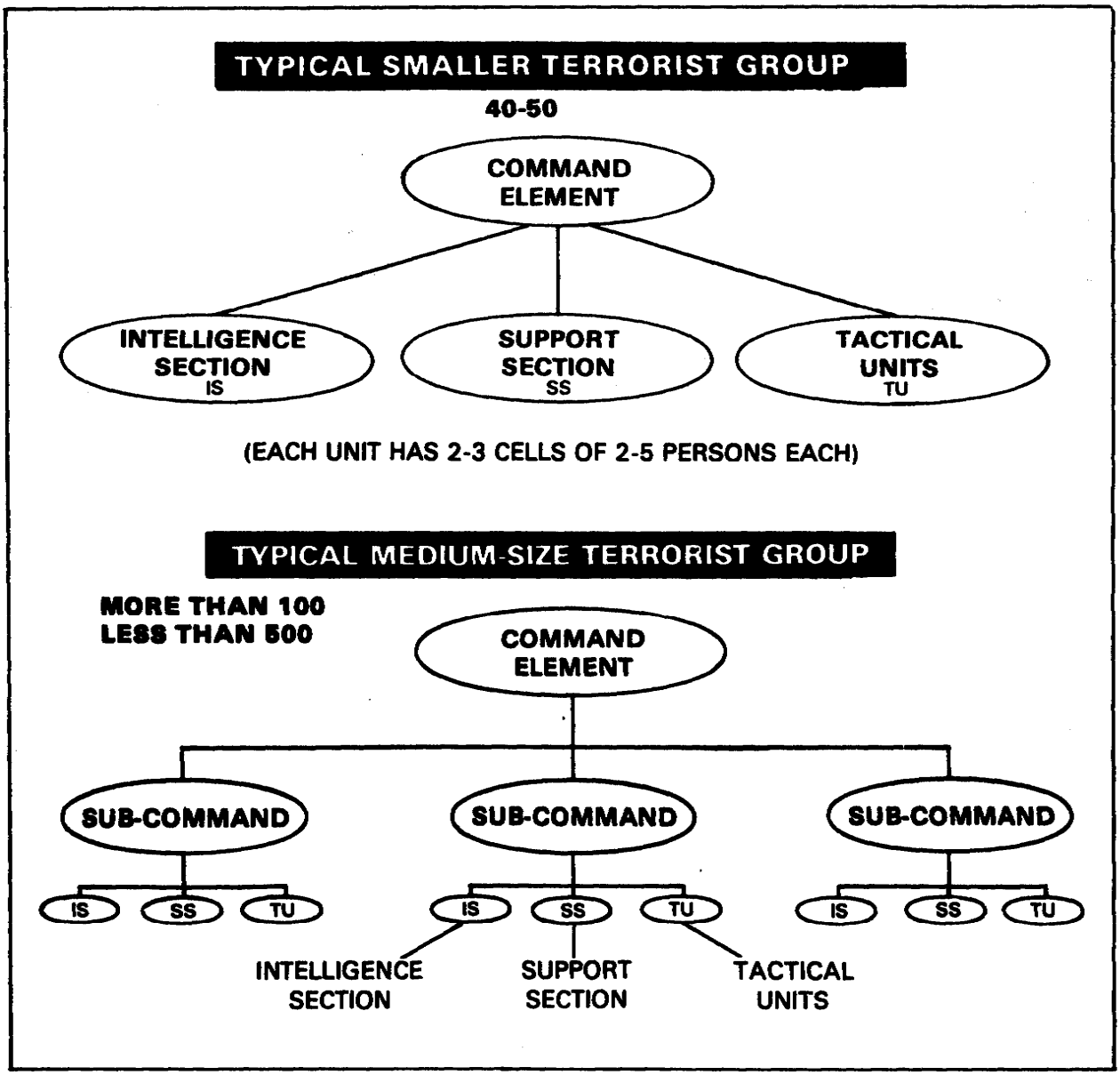


Figure 3-4. Cellular Structures.

PART E: CRISIS MANAGEMENT AND THE THREAT COMMITTEE

Recent increases in the number of terrorist acts and hostage situations make it essential that MPs are prepared to provide protection, and control these types of situations. Because these acts are often well-planned and coordinated, it is essential that all MP personnel understand their role and perform their duties as well as possible. Special threat situations must be handled promptly and efficiently to minimize loss of life and property damage.

1. Crisis Management.

Crisis management can be defined as plans, procedures, techniques, policies, and controls for dealing with terrorism, special threats, or other major disruptions, occurring on government property.

Crisis Management has two phases: the proactive phase and the reactive phase. The proactive phase includes the planning of preventive measures, preparation, and training prior to a terrorist incident. During this phase, consideration is given to research, information and intelligence planning, employment of preventive measures, in-depth planning, and extensive training.

The reactive phase is the response to increased threat levels and the management of a terrorist incident or incidents. The U.S. Army Military Police School (USAMPS) model (Figure 3-5) displays these proactive and reactive areas.

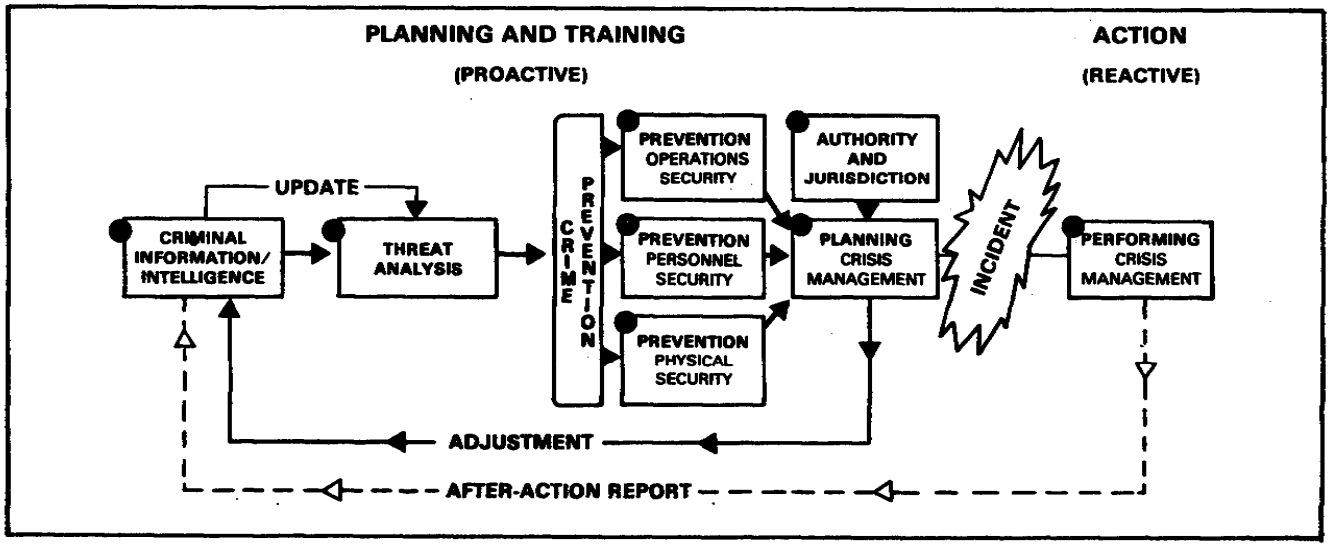


Figure 3-5. Combatting Terrorism.

Studies of terrorist's methods reveal that the best chance of success against terrorism lies in the proactive phase. Well-planned prevention is the best defense against terrorism.

The installation must plan to prevent a terrorist incident, and to make the initial response should a terrorist incident occur. Rudin's Law states that in time of crisis most people will choose the worst course of action possible. This is not due to incompetency, but a lack of enough information on which to base a decision. Proper crisis management does not mean management by crisis.

Crisis Management is a detailed, rehearsed plan to prevent and deal with special threat scenarios that all key personnel must be familiar with. Using the USAMPS model will help ensure that your counterterrorism plan is successful.

2. The Ad Hoc Threat Committee.

The ad hoc threat committee meets quarterly or as the situation dictates. They share intelligence data to help predict and prepare for special threat situations. As the committee that performs the crisis management for the installation, they should also perform as the crisis management team during a real terrorist incident. As a minimum, the committee should be composed of the Chief of Staff or Director, Plans, Training, and Security (DPTSEC), and primary installation staff personnel. The Chief of Staff or DPTSEC chairs the committee. He is in charge of scheduling times and frequency of meetings, emergency sessions, and facilities. Key personnel are from FBI, CID, physical security and counterterrorism, G2/military intelligence, and G3/operations. The ad hoc threat committee is an indispensable tool in developing liaison and a working coordination with all post and civilian counterparts. They should be combined with other committees, such as the crisis management team, to make decisions from a single efficient source. To prepare for special threat situations, the committee must conduct a threat analysis to identify the potential threat. They should have tasking authority to be fully effective.

3. Threat Analysis.

A threat analysis is a total evaluation of all possible information to determine the security posture of the installation. The analysis is done with regard to the various threats, targets, and weaknesses.

When conducting a threat analysis, you must think like a terrorist. Look around your installation. Ask yourself questions that a terrorist would ask. How would you attack your own installation? Consider areas that are vulnerable and that would attract publicity if attacked. Consider previous terrorist operations that have been successful. What did the terrorist use as targets? Thinking like a terrorist will help you to identify the area you must protect.

War games can help to identify installation weaknesses. Develop various attack scenarios with your threat committee. Field exercises using small MP

units can also be used to provide examples that can help your committee analyze possible threats.

4. The Installation Vulnerability Determining System (IVDS).

To help in determining the vulnerability of an installation to a terrorist threat, the IVDS system was created. Combined with crime prevention physical security surveys and terrorist threat intelligence, IVDS can provide the installation commander and/or the threat committee with a guide to potential installation vulnerabilities.

The following factors are reviewed to determine the installation vulnerability:

- o Installation's characteristics and its attractiveness as a target for terrorist acts.
- o Status of training.
- o Availability of communications.
- o Civilian law enforcement resources.
- o Time and distance from U.S. military installations able to lend assistance.
- o Time and distance from urban areas.
- o Geographic region.
- o Proximity to foreign borders.
- o Access to installation.
- o Population density.
- o Terrain.

The IVDS system uses a scale of 0 to 100 points. Points are assigned for each factor. The higher the value, the higher the assessed vulnerability. It must be remembered that no factor is a determinant by itself. The relationship between factors must be considered also.

There are two factors that an installation commander or PM can significantly influence to reduce the vulnerability level of the installation.

- o Attitude of Area Population.
- o Law Enforcement Resources.

Attitude of Area Population. The vulnerability value for area social environment can be greatly reduced. The installation commander and/or the PM should be an active member, on a regular basis, in meetings or on councils with other area law enforcement agencies. There are restrictions on federal authorities for collecting domestic intelligence. However, these restrictions do not apply to criminal information. Close contact with state and local authorities is the best way to stay current on the social environment around the installation. Participation in community activities and good relations with civic organizations will also create favorable attitudes in the area.

Law Enforcement Resources. Wise use of military law enforcement assets can reduce the vulnerability value of the local law enforcement factor. This can be done by training and use of counterterrorism equipment. Special training for countersnipers, special reaction teams, and hostage negotiators, give added flexibility to law enforcement personnel and to the commander. Cooperations and exchange training programs with civilian law enforcement agencies will help. (Consult AR 500-50, paragraph 304, for guidance before training with civilian agencies. It will be available at your post.) The counterterrorism management officer or NCO should encourage attendance at special training courses and schools. Civilian law enforcement agencies might agree to provide more patrolling around the outside of the installation during high-threat periods or actual incidents. This could relieve limited resources within the installation to provide more internal security for perceived targets. A good working relationship with local law enforcement agencies can provide distinct advantages and benefits.

Threat analysis is a continuous, ongoing function. Vulnerability may increase or decrease in areas in the course of normal operations. Failure to update your installation assessment on a regular basis seriously restricts your terrorism counteraction capabilities.

PART F: THE U.S. POLICY ON TERRORISM AND THE LEAD AGENCY CONCEPT

The U.S. policy on terrorism is summarized below.

- We condemn all terrorist actions.
- All lawful measures to prevent such actions will be taken.
- The U.S. will not bargain with terrorists.
- We will continue to cultivate international cooperation to combat terrorism.

1. Procedures Inside the Continental United States (CONUS).

The Department of Justice and the FBI in particular, has primary law enforcement responsibility for terrorist incidents in the United States, including the District of Columbia, the Commonwealth of Puerto Rico, and U.S. possessions and territories. The installation commander has responsibility

for the maintenance of law and order on the installation.

Within the United States, the installation commander will provide the initial and immediate response to any incident occurring on a military installation, but the FBI will be notified immediately. They will assume jurisdiction if it is determined that such an incident is of significant Federal interest.

The following procedures are to be taken in response to terrorist incidents on a military installation:

a. "Installation" security forces will isolate, contain, and neutralize (if the situation dictates).

b. The FBI will be notified. They will determine jurisdictional responsibility.

c. The senior FBI official will establish liaison with the command center at the installation. He will coordinate the use of FBI assets to assist in resolving the incident.

d. If the FBI declines jurisdiction, they may act in an advisory role to military authorities in resolving the situation.

When the FBI declines jurisdiction, the military will take action to resolve the incident. Even if the FBI assumes jurisdiction, the military commander may take immediate actions, as dictated by the situation. This will be to prevent loss of life or property damage before the FBI response force arrives.

Teamwork and cooperation must be stressed in a terrorist incident. Close liaison between the senior FBI official and the installation commander is essential to determining jurisdiction and resolving the terrorist incident.

2. Procedures Outside the United States (OCONUS).

The State Department will often have primary responsibility for dealing with terrorism involving American's abroad and for enhancing the security of all U.S. Government personnel overseas. However, the host government, as per Status of Forces Agreement (SOFA) or the Memorandum of Agreement or Understanding, has primary responsibility for managing terrorist incidents within that nation. Reference must be made to each individual SOFA. Contingency plans will address the use of installation, military, and host nation forces. This will be coordinated with both host country and State Department officials.

The use of host nation resources instead of U.S. forces will be determined through SOFA or other agreements.

PART G: DEFINITION OF SPECIAL THREAT AND DEVELOPMENT OF THE SPECIAL THREAT PLAN

1. Definition of Special Threat.

A special threat is any situation involving a sniper, barricaded criminal(s), terrorist activity/major disruptions, or hostage taker(s), that is beyond the capacity of standard police equipment, manpower, and training. All special threat situations pose a grave danger to hostages, bystanders, and law enforcement personnel. Locations, motivations, responses and other circumstances will differ. Special threat situations must be dealt with on an individual basis. Law enforcement response must be clear, decisive, and coordinated. The safety of any hostages and their release without injury is an important consideration and must be weighed against the circumstances of the situation. To deal with these situations, a special threat plan must be in place at each installation.

2. Development of the Special Threat Plan.

The special threat plan is prepared in coordination with the installation staff. The plan must assign specific duties and responsibilities to identified personnel. (It will normally be produced as an annex to the installation crisis management plan, which will also cover situations outside the narrow scope of a "special threat.") It must include circumstances that activate the team, notification procedures, and operational procedures to maximize effectiveness. Get the first team behind the special threat plan. Your best personnel will be needed in times of crisis. Continual intelligence updates along with regular training and practice of the special threat plan will ensure that it is effective if and when you must use it.

Development of the special threat plan requires that you implement the proactive (preventive) practice phase of the USAMPS terrorism counteraction model (see Figure 3-5).

This phase contains the following elements:

a. Criminal Information/intelligence.

b. Threat analysis.

c. Operations security.

d. Personnel security.

e. Physical security.

f. Authority and jurisdiction.

g. Crisis Management Planning (final development of special threat plan).

3. Criminal Information/Intelligence.

Information must go through two stages: Collection and Analyzation/Dissemination.

Collection. Information gathering is of primary importance in any examination of terrorism. The first task is to determine what data is needed to develop an adequate terrorism counteraction program. Knowledge is power. The more knowledge you have about your adversaries, the better equipped you will be to counter their activities. There is more information and intelligence available than a single installation would need or be able to store. You must develop a system that tells you who has what information, and how you can obtain it when you need it.

There are three potential sources for information: Open sources, criminal information, or the pure intelligence field.

Open Sources of Information:

- Commercial publications.
- Schools and seminars.
- Installation library.
- Media (newspapers and television).
- College professors.
- CIA, FBI, State Department's Office for Combatting Terrorism, and National Criminal Justice Reference Service.

Criminal Information

- Provost Marshal.
- Military Police Investigators (MPI).
- U.S. Army Criminal Investigation Command (USACIDC) agents.

When using sources of criminal information, do not attempt to set up sources without going through existing local contacts. Going outside of established information routes may violate existing confidential relationships.

Intelligence

- U.S. Army Intelligence School.
- Working field agents.

NOTE: Classified information may prevent some intelligence from reaching MPs or local law enforcement agencies. It is because of this that the sharing of intelligence at Threat Committee meetings is so important, as it allows the user and not just the analyst to benefit from the information.

Analyzation/Dissemination. The new data must be compared with existing data. This will help to determine new trends and to identify terrorist individuals and groups. Determine if it is pertinent, reliable, and/or applicable. The information is disseminated by the most secure and expedient methods possible. To disseminate data rapidly, keep it in unclassified format whenever possible. This will ensure the greatest distribution of data. Information intelligence must be in the hands of the command authority in time to be used.

Crime Prevention: Operational, Personnel, and Physical Security Crime prevention is an essential element to the proactive phase of counterterrorist planning.

Operational security. The security of day-to-day operations is easily overlooked. Operational security (OPSEC) is vital to the strength of your installation. The security of communications system information activities and human communications should be closely examined. Counter-surveillance techniques must be used when possible. Information learned about terrorists can provide firsthand knowledge about potential targets. The basic objectives of operational security are described below.

Avoid stereotyping operations. Changing procedures on a random basis confuses a potential adversary. The degree of randomness can be increased by changing patrol routes on different days of the week. Change patrol schedules, or assign personnel to different areas and shifts.

Understand techniques used by terrorists to collect intelligence. These are displayed in Figure 3-6.

Protect information. It is the cornerstone of the OPSEC program. It is essential to prevent terrorists from discovering or buying information which could be of value to them in planning an attack.

4. Personnel Security.

Terrorists select specific people as targets for kidnapping, extortion, hostage-taking, and assassination. They may be selected as a target by their rank or for their knowledge. The objectives of personnel security are to develop programs which include planning, education, and awareness.

These programs help to inform as many people as possible of the terrorist threat. This can be through briefings, seminars and presentations on and off-post. A partial list of personal preventive measures is included below:

- o Preventing direct access by the public to sensitive areas likely to be targets of terrorism. For instance, command office areas should be located above the ground floor level.

- o Equipping the place where visitors enter command offices with a duress alarm.

- o Ensuring visitors are escorted and their access into sensitive or command office areas is controlled. This is a key element of a security policy.

- o Making a careful examination of all measures used to control the entry of persons into sensitive or command office areas during nonworking hours; directing the security force to make periodic checks of command office areas during their after-hours tours.

TECHNIQUE	ACTIVITIES	COUNTERMEASURES
HUMINT	CASUAL CONVERSATIONS, PLANTING AGENTS.	TRAINING PERSONNEL, COUNTERSURVEILLANCE, AND COUNTERINTELLIGENCE.
SIGINT	INTERCEPTION OF COMMUNICATION SIGNALS.	COMMUNICATIONS SECURITY AND INFORMATION SECURITY.
PHOTINT	PHOTOGRAPHING ACTIVITIES FROM AIRCRAFT, HIGH TERRAIN, OR AUTOMOBILE.	COUNTERINTELLIGENCE, COUNTERSURVEILLLANCE, AND ACCESS CONTROL.
OPERATIONAL PATTERNS	OBSERVING STEREOTYPED OPERATIONS.	RANDOMIZE OPERATIONAL PATTERNS; EMPLOY DECEPTION.

Figure 3-6. Terrorist Intelligence Collection.

- Ensuring all restrooms on floors where command offices are located (and all restrooms in a multistory office building) are locked after duty hours to eliminate public access.

- Ensuring doors to janitorial and other maintenance closets are kept locked at all times.

- Ensuring doors to telephone and electrical equipment rooms are kept locked. Access is given to maintenance and telephone personnel only when they have need for such access.

- Considering selection of an interior saferoom to be used if terrorists attack. It should not be identified to the public as a saferoom.

- Maintaining emergency supplies, such as first-aid equipment, bomb blankets, food rations, candles, lanterns, and other equipment considered necessary. Make sure key personnel know where the supplies are kept and the locations of emergency exits and escape routes.

- Restricting the release of personal data on key personnel. This is used by terrorists to select victims or identify their homes and families.

- Recommending that key personnel parking areas not be identified as such. Parking spaces can be identified by number rather than by name or title.

- Limiting information on travel itineraries and arrangements for command or key personnel to as few people as possible. Code names and assumed names may be required under special circumstances. Consider making itineraries "for official use only" (FOUO), and number them. This provides accountability and responsibility.

- Increasing the effectiveness of protective measures for command and key personnel by encouraging them to--

  - maintain a low profile.

  - learn to recognize signs that they may be under surveillance. Being constantly aware of their environment can be their most effective prevention tool.

- Use simple verbal code signals to alert family or organization members to a physical threat.

- Conduct crime prevention surveys of on-post activities to reduce the likelihood and opportunity for crimes to occur.

- Protect very important persons (VIPs) and high risk personnel (HRPs). Provide personnel security to high risk people through personal security missions and protective services details.

Physical Security. Physical security measures protect buildings, people and information against criminal acts. The objectives are to develop physical security plans, surveys, and/or inspections. These plans should ensure that the intrusion detection system is supported by a security guard force that can apprehend intruders or prevent entry by unauthorized persons. In addition, permanent or temporary restricted areas should be set up along with the allocation of MPs. Previous inspection surveys and physical security checks should be analyzed and updated. Develop overall threat considerations and goals for the installation.

PART H - TERRORISM COUNTERACTION CRISIS MANAGEMENT PLAN

The plan format can be adapted to any particular situation. It should, however, contain the key elements of the plan. These should include:

- The organization - what is the chain of command?
- The installation situation - what is the status of the terrorist forces compared to yours?
- The installation mission - what are the overall goals of the installation?
- Execution of the mission - what is the specific tactical plan against terrorism?
- Service support - how will the men and material be coordinated?
- Command and signal - what are the communications methods and equipment to be used?

Terrorism Counteraction Special Threat Annex to the Installation Crisis Management Plan

REFERENCES: Maps, charts, and other relevant documents.

TIME ZONE USED THROUGHOUT THIS PLAN:

TASK ORGANIZATION: Contains a listing of units organized to conduct a counterterrorism operation. It includes attachments, supporting roles, and delegation of operational control as necessary.

1. SITUATION: Contains information on the general situation in order to understand ongoing events influencing the counterterrorism response.

a. Terrorist Force. Contains information about terrorist composition, disposition, methods of operation, estimated strength, and capabilities which could influence the counterterrorism operation. Usually this information is provided in a referenced annex, if published or to be published--e.g., Annex A (Intel).

b. Counterterrorist Force. Contains pertinent information about our forces that could directly influence the counterterrorism mission. Do not repeat information included elsewhere in the plan.

c. Attachments and Detachments. Self-explanatory (may be written here or as a referenced annex).

d. Assumptions. Contains those applicable as a basis for this plan (for example, strength of counterterrorism force to be supported or support available from other agencies).

(1) Tactical situation possibilities. Obtained from the commander's planning guidance.

(2) Personnel situation. Provided by the personnel officer.

(3) Logistic situation. Provided by the logistics officer.

(4) Legal situation possibilities. Provided by the Staff Judge Advocate.

2. MISSION: Contains a statement of the terrorism counteraction mission(s) on the installation as a whole. An example would be… "to contain and neutralize special threats and actions aimed at the disruption of this installation."

3. EXECUTION:

a. Concept of Operation. Contains a statement of the commander's tactical plan. Its purpose is to inform. It may also state, where needed, how he envisions the conduct of the operation and perceives its purpose. Although it should be brief, give enough detail to ensure proper action by subordinates in the absence of other specific instructions.

(1) An operation may involve two or more distinct phases. This will normally be the case in a terrorism counteraction operation. Designate each phase and use subparagraphs to describe each one (Phase I, Phase II. . .).

(2) The concept of the operation, if very long, may appear as an annex.

b. In subsequent separate lettered subparagraphs, give the specific task(s) for each element of the command charged with executing a terrorism counteraction mission. When giving multiple instructions, itemize them and indicate any priority or sequence (e.g., Commander, 000th MP Co will be prepared to provide a one platoon ready reaction force).

c. Coordinating instructions. The last subparagraph of paragraph 3 contains the details of coordination and control that apply to two or more elements of the command (this plan is effective for planning on receipt,

implementation on order, or units with designated security mission to submit operation plans to this HQ for approval).

4. SERVICE SUPPORT: Contains a statement of service support instructions and arrangements supporting the counterterrorism operation. These are of foremost interest to the committed elements. If it is long, it may be included as an annex and referenced here; however, make sure matters of immediate concern are given in the reference. The following subparagraphs are used, as required:

a. General. Outline of the general plan of service support.

b. Material and Services.

(1) Supply.

(2) Transportation.

(3) Services. Contains information and/or instructions for the supported elements that prescribe the type of service available. It also contains the designation and location of the unit, and schedule of service if applicable.

(a) Engineer support.

(b) Health services: medical hold, blood control, etc.

(c) Installation service: fire protection, water supply, utilities.

(4) Labor. Contains policies pertaining to civilian work force.

(5) Maintenance. Contains priorities of maintenance, location of facilities, and collection points.

c. Medical Evacuation and Hospitalization. Prescribes the plan for evacuation and hospitalization of sick, wounded, or injured personnel. Include responsibilities for evacuation and specific policy for evacuation by air.

5. Personnel. Contains information and instructions for supporting units pertaining to personnel. It also contains installation activities, and place and time of opening or closing.

(1) Maintenance of unit strength.

(a) Strength Reports. Contains instructions for submitting data needed to inform the commander on the status of strength. Includes requirements for routine and special reports.

(b) Replacements. Contains a statement validating existing personnel requisitions, instructions for submitting requisitions, and instructions for processing and removing replacements.

(2) Personnel management.

(a) Military personnel.

(b) Civilian personnel.

(c) Civilian detainees. Indicate disposition for apprehended terrorist(s).

(3) Development and maintenance of morale.

(a) Morale and personnel services. Contains information and/or instructions about postal and finance services, religious activities, personal hygiene, and special services activities.

(b) Graves registration. Includes evacuation procedures, and handling of personal effects.

(4) Maintenance of discipline, law, and order.

(5) Miscellaneous. Includes personnel administrative matters not specifically assigned to another coordinating staff section or included in the preceding subparagraphs.

a. Miscellaneous. Contains special instructions not covered above.

(1) Special reports. Include those reports required, but not included, in previous paragraphs, or those requiring special emphasis.

(2) Other information and/or instructions not included in any previous paragraph.

6. COMMAND AND SIGNAL: This contains instructions for command and operation of communications-electronic (C-E). This paragraph may have as many subparagraphs as needed. Two of the more common subheadings are "Signal" and "Command." C-E instructions may refer to an annex, but, as a minimum, should list the index and issue number of the C-E operation instructions (CEOI) in effect. If not already issued, give instructions for control, coordination, and establishment of priorities in the use of electromagnetic emissions. Command instructions include command post (CP) location of subordinate and higher units. Designation of alternate CP and succession of command will be entered in this subparagraph, if not covered in SOP or annex.

ACKNOWLEDGEMENT INSTRUCTIONS:

(Last Name of Installation Commander)

(Rank of Commander)

/s/(Last of operations officer)

LAST NAME OF THE OPERATION OFFICER (typed)

G3

ANNEXES: List appropriate annexes here.

DISTRIBUTION: List those elements of the command who will receive copies of the plan. Make appropriate notation and copy number on page 1.

PART H: DESCRIBE THE ESTABLISHMENT OF AN INSTALLATION CRISIS MANAGEMENT TEAM

The crisis management team (CMT) is a staff team set up to plan, coordinate, and draft special threat plans. The CMT usually operates from the emergency operations center (EOC) during a terrorist incident. The commander of the CMT is usually the deputy installation commander or alternatively the chief of staff.

The CMT is also responsible for setting up the threat management force (TMF). The TMF is the tactical element of the CMT that physically responds to major installation disruptions.

A recommended crisis management organization is shown in Figure 3-7.

The CMT is made up of representatives of various military staff sections. They advise the CMT commander in their areas of expertise. Representatives and their responsibilities are detailed below.

PMO SECURITY FORCE COMMANDER - Provost Marshal - He activates and coordinates the law enforcement response. He controls all access to and from the installation, and informs the installation commander of all developments. He establishes and maintains contact with all other elements; this includes the FBI, local law enforcement, and CID. He controls access and egress of installation and advises the CG on all developments.

Chief of Staff - The Chief of Staff usually maintains control of other installation activities during a terrorist/special threat incident.

G1 - Adjutant General - He provides information on personnel involved.

G2 - Military Intelligence - He provides information and intelligence on terrorists.

G3 - Operations - Provide overall staff coordination for terrorism counteractions, and ensure that proper operational responses are taken in order to protect the installation.

G4 - Director of Logistics - He is in charge of transportation, supply, and maintenance, and makes local purchases if necessary.

SJA - Staff Judge Advocate - He provides legal guidance as to the proper exercise of authority and jurisdiction.

PAO - Public Affairs Officer - He establishes a press center and deals with all media and media personnel.

DCE - Communications - He handles all communications requirements to teams, hostages, terrorists, and law enforcement personnel.

Engr - Engineers - They provide information on facilities and any engineering support.

Other elements:

SRT - Special Reaction Team. A specially trained team armed and equipped to neutralize a special threat to the installation. Controlled by the TMF commander.

Neg Team - Hostage Negotiation Team. They initiate dialogue between authorities and offender in an attempt to gain intelligence. They stall for time, and/or cause the surrender of the offender.

PART I: DESCRIBE THE MANAGING OF A SPECIAL THREAT INCIDENT

There is no particular method of operation that can be used in every situation. Every terrorist incident is different. It must be managed according to its unique problems. The following outline provides a model of actions to be taken in response to special threats. Response to a terrorist incident generally occurs in three phases.

Phase 1 involves a commitment of local resources, essentially the MP, to the scene. It is important that other MP patrols remain in the areas assigned to them. The initial incident may be a diversionary tactic to pull security forces away from the target. These patrols should be aware of sensitive or high-risk potential targets in their area. They must make sure those targets are secure.

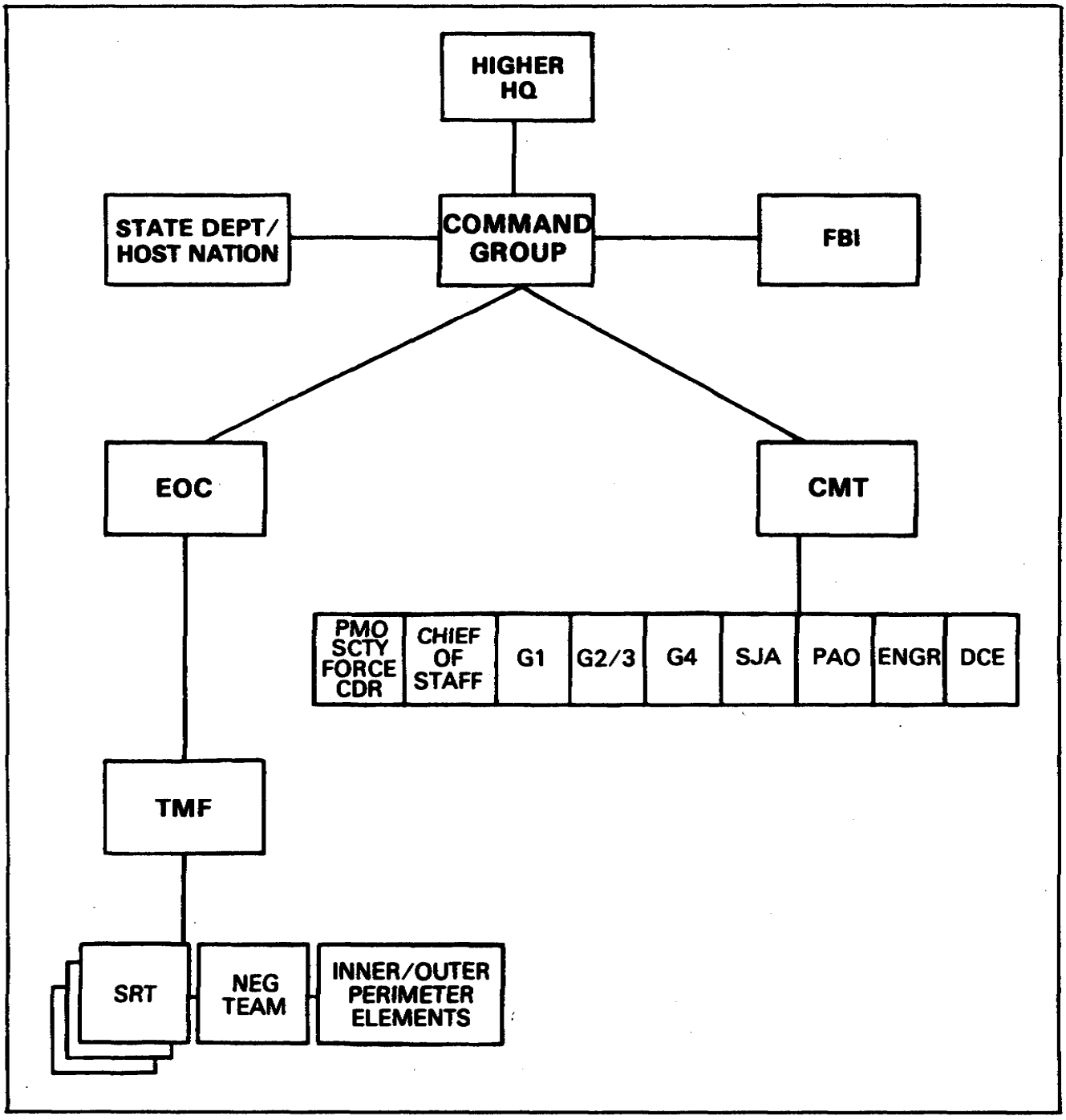


Figure 3-7. Crisis Management Organization.

Phase 2 is enhancement of the initial response force by the TMF, FBI, or host-nation units. This phase begins upon notification of the EOC and activation of the CMT.

Phase 3 is the commitment of the Department of Defense or host-nation counterterrorism force. This is the phase in which steps are taken to terminate the incident.

The use of resources may extend from one phase to another. For example, the initial MP patrol on the scene (Phase 1) may be assigned to the TMF that assumes control during Phase 2. They may also be involved in providing inner-or outer-perimeter support during Phase 3.

The steps contained in each phase are detailed below.

Phase 1 - Response of local forces within installation.

1) Incident spotted.
Second party report.
Personal observation.

2) Dispatch appropriate law enforcement response.
Request reinforcements.

3) Estimate of situation.
Situation report.

4) Isolate and contain incident.
Evacuate friendly personnel.
Establish inner and outer perimeter.

5) Gather information.
Identification and contact of terrorists.
Supplemental situation report of Desk SGT.

6) Activate Special Threat Plan - EOC, CMT, TMF.
Operationally establish think tank, field command post.

IF CONUS - Notify AOC by fastest means possible. Notify FBI - if there is a significant federal interest, FBI responds.

7) If the incident is determined as not of significant federal interest, or host/nation does not respond, the local installation must resolve the incident.

Phase 2 - FBI or Host nation enhances response.

1) FBI, Host nation counterterrorist forces respond.

2) Installation commander retains command/control of his assets.

3) Resolve at law enforcement level or escalate.

Phase 3 - National Command Authority/DOD Counterterrorism joint task force responds.

1) IF CONUS - When action is beyond FBI's capabilities and action is justified, National Command Authority commits the DOD counterterrorist force.

2) IF OCONUS - When action is beyond host nation law enforcement or host nation counterterrorist force and they request additional U.S. assistance, the National Command Authority may commit the DOD counterterrorist force.

1. Responding to the Tactical Situation.

An ongoing terrorist incident must be treated as a tactical situation, with certain differences for the terrorist situation. An installation could be faced with a bombing, an assault/ambush, hijacking, kidnapping, a hostage/barricade or arson, or any combination of the above.

2. Bombings.

If the terrorist plants bombs, then you must assume other bombs have been planted. Alert the bomb search teams and the EOD personnel. The initial response force removes everyone from the scene to a safe area. Anyone near the scene at the time of the explosion is interviewed. Keep in mind that the people being interviewed may, in fact, be the terrorists who planted the bomb. Suspected devices are checked by EOD personnel. Once search is completed, the crime scene investigation begins at the bombing site. Normal security is resumed at other locations.

3. Ambush/Attack

Always assume the terrorists are still in the area. The initial response force renders aid to the victims and establishes a defensive perimeter. When reinforcements arrive, they normally clear the area before the crime scene investigation begins or normal activity is resumed. Use all available resources, including aircraft, when clearing the area. Exits from the post must be controlled as soon as a terrorist event takes place. The terrorists may still be on the installation. Vehicles leaving the post must be inspected and personnel identified. The MPs securing post exits must also be alert for possible ambushes. Once security is established, allow only mission essential personnel to enter the post until the initial response to the incident is complete.

4. Hijacking.

When a hijacking/skyjacking occurs, the initial response force attempts to contain the situation. They try to prevent the terrorists from taking off when they are in an aircraft, or from going mobile when they are in a ground

vehicle. Once activated, the TMF continues to contain the incident, unless otherwise directed by the EOC. The main counterterrorism objectives during a hijacking/skyjacking are to contain the situation. They either negotiate with the terrorists or terminate the incident through a successful assault. If you have aircraft at your installation, your TMF and special reaction teams should rehearse assaults on aircraft to be familiar with this type of operation. However, it may be best to allow a highly trained and specialized team, such as an FBI or host nation force, to make the assault. Use the military police SRT to make the assault only as a last-ditch effort.

5. Kidnapping.

In most cases of kidnapping, you will not be aware that it has occurred until the terrorists have the victim safely secured elsewhere. The immediate response is to dispatch MP patrols to provide protection for other possible targets. This includes members of the victim's family. Activate the CMT. The CMT can materially aid the commander in dealing with the kidnapping. They can help coordinate military support, make reports to higher headquarters, develop news releases, and recommend possible courses of action (the TMF may be placed on alert if the commander feels there is a need). During a kidnapping, the TMF is not normally committed.

USACIDC personnel will investigate the scene of the abduction. The SRT is ready to activate if the victim or terrorists are located on the installation. At this point, the hostage negotiation team assumes an active role. They can be dedicated directly to the EOC and are responsible for direct communications with the terrorists, if that is necessary.

6. Hostage/Barricade Situation.

The worst possible scenario you could be confronted with is a prolonged hostage/barricade situation. If you have a prolonged event, do you continue normal operations on the rest of the installation? Which assets should be committed to managing the incident, and how will that affect other operations? Assuming the Army maintains control over the incident and decides to commit higher level special reaction forces; where would they land; how would they be transported to the incident site; and how would they assume control or effect the passage of lines? Remember, the military always remains in control of its troops. The jurisdiction for the incident may be assumed by another agency or by the host nation, but the installation continues its security. This includes its inner- and outer-perimeter security mission, gate security missions, and similar security functions for an ongoing terrorist mission. The installation EOC/CMT/TMF continues to function, even after handoff of jurisdiction has taken place.

7. Arson.

Terrorists use incendiary devices to commit arson. This is often done during an organized civil disturbance (throwing a fire bomb), or against a targeted building. They also use such devices to destroy vehicles. As with bombs, they often use time delay mechanisms to allow themselves time to leave the

area before the fire occurs. They booby-trap buildings with grenades to increase casualties among firefighters responding to the scene. Firefighters and MP patrol personnel must be aware of this tactic and be alert to potential booby traps. Terrorists may set secondary devices, including bombs, for a time delay detonation. The area must be secured during fire suppression. It must be inspected by a bomb search team and EOD personnel before beginning a crime/fire scene investigation.

LESSON 3

PRACTICE EXERCISE

This practice exercise is designed to test your knowledge of the material. This lesson covered the required material to plan/conduct terrorism counteraction activities on a military installation. To check your understanding of the lesson, complete the practice exercise below. All of the questions are multiple-choice with one correct (or best) answer. Try to answer all the questions without referring to the lesson material.

When you have answered all of the questions, turn the page and check: your answers against the answer key. Review any questions you missed or don't understand. When you have completed your review, continue to the next lesson.

1. You are instructing a group in terrorism history, and you explain one of the factors that makes modern terrorism much more dangerous then pre-modern terrorism. Which would you explain?

A. More people have difficulties dealing with stress.
B. Today's technology is capable of more powerful weapons.
C. More people are bilingual.
D. The formation of OPEC.

2. To prepare for a terrorist incident, you must defend against the terrorism tactic most common to terrorist groups. Which is the most common?

A. Arson.
B. Kidnapping.
C. Bombing.
D. Hijacking.

3. You refer to the typical "medium-size" terrorist group as having how many members?

A. 40-50 members.
B. 50-100 members.
C. 100-500 members.
D. 1000-5000 members.

4. As commander of your military installation, you are aware that the best defense against terrorism is:

A. well-planned prevention.
B. a good offense.
C. large amounts of men and weapons.
D. communication with the terrorists.

5. As installation commander, you usually delegate the task of coordinating special threat planning to the:

A. Chief of Staff.
B. Deputy installation commander.
C. Provost Marshal.
D. G3 operations.

6. You are the installation commander OCONUS and a terrorist incident occurs on your base. The primary U.S. responsibility for managing that incident goes to the:

A. FBI.
B. CIA.
C. Military installation.
D. Department of State.

7. You are on the threat committee and you are establishing a criteria for information/intelligence on terrorism. Your priority is to:

A. compile a computer bank with all available information.
B. compile an installation library.
C. develop a system that enables you to find what you need when you need it.
D. maintain a staff of terrorism counteraction experts on-base.

8. The FBI has assumed jurisdiction over your installation incident and has responded with force. As installation commander, you:

A. retain control of your assets and engage terrorists, if requested.
B. give control of your assets to the FBI senior officer.
C. never engage your own personnel in an incident the FBI has assumed jurisdiction over.
D. move in without consultation if the situation is undecided.

LESSON 3

PRACTICE EXERCISE

ANSWER KEY AND FEEDBACK

Item		Correct Answer and Feedback
1.	B.	Today's technology is capable of more powerful weapons. The potential for superviolence . . . (page 3-3, para 4).
2.	C.	Bombing. The tactic most common . . . (page 3-5, para 1).
3.	C.	100-500 members. The diagrams in Figure 3-4 represent . . . (page 3-9, para 4).
4.	A.	Well-planned prevention. Studies of terrorist methods reveal . . . (page 3-12, para 1).
5.	D.	G3 operations. Key personnel are from . . . (page 3-12, para 2).
6.	D.	Department of State. The State Department will . . . (page 3-15, para 2).
7.	C.	Develop a system that enables you to find what you need when you need it. There is more information and . . . (page 3-17, para 3).
8.	A.	Retain control of you assets and engage terrorist, if requested. When the FBI declines jurisdiction . . . (page 3-15, para 1).

The Army Combatting Terrorism Program

(12) Publish DA Force Protection Travel Advisories, as required, to inform commanders of DoD-designated high and potential physical threat countries, high crime rate cities and DoS Travel Advisories.

(13) Maintain a master file of all personnel designated HRP I by commanders of MACOMs.

b. Operate an Antiterrorism Operations and Intelligence Cell (ATOIC) in conjunction with the ODCSINT in the Army Operations Center (AOC) to monitor and report worldwide threat conditions (THREATCONs), analyze terrorist-related intelligence and review criminal information in order to provide early warning of terrorist threats to MACOMs, the senior Army leadership, and threatened installations, activities and facilities.

Chapter 2
Responsibilities

2–1. Director of the Army Staff (DAS)

The DAS is responsible for designating High Risk Personnel (HRP) within the Military District of Washington, per AR 190–58 and paragraph 3–12 of this regulation.

2–2. Deputy Chief of Staff for Operations and Plans (DCSOPS)

The DCSOPS is responsible for the security of the Army and provides overall policy guidance and staff supervision and coordination for the Army CBT/T Program. In discharging overall general staff responsibility for the Program, the DCSOPS will—

a. Assign a full-time program management element to—

(1) Serve as the Army CBT/T focal point for coordination with DoD, Organization of the Joint Chiefs of Staff (OJCS), the other Services, Defense agencies, and major army commands (MACOMs).

(2) Represent HQDA on appropriate committees and forums.

(3) Establish Army CBT/T policy and objectives, coordinate policies and procedures consistent with DoD Directives, and provide resources.

(4) Review CBT/T plans and reports to ensure program effectiveness.

(5) Integrate foreign intelligence, counterintelligence, criminal information, operations security (OPSEC), physical security, and law enforcement activities into CBT/T planning and practice, with the assistance of the Office of the Deputy Chief of Staff for Intelligence (ODCSINT) and other intelligence, security and law enforcement agencies, as appropriate.

(6) Evaluate the Army CBT/T posture and the effectiveness of command CBT/T programs, and provide guidance and assistance, as required.

(7) Coordinate resource requirements for staffing and administering command CBT/T Program functions.

(8) Establish policy governing development of CBT/T doctrine and training.

(9) Review CBT/T doctrine and training to ensure conformity with national, DoD, and Army CBT/T policy and guidance.

(10) Develop and evaluate policy and procedures for law enforcement and physical security matters pertaining to the CBT/T Program.

(11) Review requests for specialized CBT/T training to ensure that allocation of school quotas supports CBT/T operational requirements.

2–3. Deputy Chief of Staff for Personnel (DCSPER)

The DCSPER will—

a. Ensure that CBT/T policies and procedures are incorporated in personnel and travel guidance, to include Army policies governing permanent change of station (PCS) and temporary duty (TDY) to designated high and potential physical threat countries.

b. Establish procedures to ensure that Army personnel who will be designated as HRP by virtue of assignment to a high risk billet (HRB) are programmed to attend the Individual Terrorism Awareness Course (INTAC) prior to reporting to such positions.

2–4. Deputy Chief of Staff for Intelligence (DCSINT)

The DCSINT will—

a. Develop policy, plans and procedures for collecting, reporting, and disseminating information concerning terrorist activities per AR 381–10.

b. Provide intelligence personnel to support operation of the ATOIC.

c. Assess the terrorist threat to U.S. Army forces.

d. Provide Army Intelligence requirements, related to terrorism, to the National Foreign Intelligence Board.

e. Represent the Army in matters related to terrorism in the Intelligence Community.

2–5. Chief of Public Affairs (CPA), Office of the Secretary of the Army (OSA)

The CPA will provide guidance for the development and execution of command information and public information programs in support of AT and CT efforts.

2–6. Chief of Engineers (COE)

The COE will—

a. Ensure that protective design measures, to include alarm systems and physical barriers, are incorporated into proposed Military Construction, Army, (MCA) projects in compliance with Army Military Construction (MILCON) policy.

b. Develop construction policies for incorporating CBT/T design measures into MILCON projects.

c. Provide administrative and technical advice and assistance and make recommendations concerning CBT/T real property matters to the Secretary of the Army; the Chief of Staff, Army; and HQDA staff agencies.

2–7. The Deputy Assistant Secretary (ASA) of the Army for Budget

The Deputy ASA for Budget will maintain a uniform tracking system to capture the expenditure of all CBT/T funds from programming through budget execution.

2–8. Chief, National Guard Bureau (CNGB)

The CNGB will—

a. Coordinate resource requirements for staffing and administering CBT/T Program functions in the Army National Guard.

b. Evaluate the CBT/T posture and the effectiveness of CBT/T Programs in the Army National Guard, and provide guidance and assistance, as required.

c. Program/budget funds and identify Army National Guard personnel for attendance at specialized CBT/T training.

d. Ensure that CBT/T design measures have been considered and included, as appropriate, in Army National Guard construction projects.

e. Establish procedures for reporting THREATCON changes implemented by Army National Guard units, facilities and activities to the ATOIC. Ensure compliance by State Adjutants General with terrorist THREATCON reporting procedures.

f. Establish procedures for dissemination of terrorist threat information to Army National Guard units, facilities and activities.

g. Establish procedures for submission of Terrorist Threat Reports (TTRs) and Terrorist Incident Reports (TIRs) by Army National Guard units.

2–9. Chief, Army Reserve (CAR)

The CAR will—

a. Coordinate resource requirements for staffing and administering CBT/T Program functions in the Army Reserve.

b. Evaluate the CBT/T posture and the effectiveness of CBT/T Programs in the Army Reserve, and provide guidance and assistance, as required.

c. Program/budget funds and identify Army Reserve personnel for attendance at specialized CBT/T training.

d. Ensure that CBT/T design measures have been considered and included, as appropriate, in Army Reserve construction projects.

2–10. Commanding General, Training and Doctrine Command (CG, TRADOC)

CG, TRADOC will—

a. Develop and implement appropriate training programs for AT, to include—

(1) An orientation for cadets and officer candidates undergoing precommissioning training and for soldiers undergoing initial entry training which familiarizes them with individual protective measures and other precautions that should be taken to protect personnel, family members, facilities, and equipment from terrorist attack.

(2) Comprehensive training in leadership courses designed to train officers and noncommissioned officers to exercise their responsibilities for protecting personnel, family members, facilities and equipment from terrorist attack, both at home station and during deployments.

(3) Specialized training for personnel assigned to operations, intelligence, criminal investigation, and Provost Marshal staff sections who have significant CBT/T responsibilities. This includes those personnel responsible for the protection HRP, and for the security of Army installations, facilities and activities; and protection of personnel and units traveling or deployed in areas where a credible terrorist threat exists; and personnel responsible for the investigation of terrorist acts.

b. Staff and resource the Army Specified Proponent for CBT/T to coordinate CBT/T doctrine and training within TRADOC and with USASOC.

c. Assist USASOC in the development of doctrine and training required to support execution of AT operations by Army Special Operations forces.

d. Develop specialized training for installation response force operations (Special Reaction Teams or SRT) and Protective Service Agents (PSA).

e. Develop doctrine, training, organization, and material for responding to terrorist acts on installations.

f. Develop doctrine, tactics, techniques, and procedures concerning individual protective measures and other precautions that should be taken to protect personnel, family members, facilities, and equipment, both on installations and during deployments.

g. Analyze and maintain a repository of lessons learned from past terrorist incidents at the Center for Army Lessons Learned (CALL).

2–11. Commanding General, U.S. Army Criminal Investigation Command (CG, USACIDC)

The CG, USACIDC will—

a. Collect, evaluate, and disseminate to affected commands criminal information pertaining to terrorist activities, within the provisions of applicable statutes and regulations.

b. Provide terrorist-related criminal information to HQDA (ATOIC), the U.S. Army Intelligence and Security Command (INSCOM) and the U.S. Army Intelligence and Threat Analysis Center (USAITAC).

c. Investigate terrorist incidents on installations and facilities, and against units, Army personnel, or their family members. Monitor the conduct of such investigations when conducted by civilian or host nation police agencies. Provide results of terrorism related investigations to HQDA (ATOIC) and CALL.

d. Provide trained hostage negotiators to support Army CBT/T operations worldwide.

e. Plan and coordinate personal protective services for DoD and DA officials, as directed by HQDA.

f. Report terrorist incidents, suspected terrorist activity and criminal information concerning the terrorist threat to appropriate local commanders.

g. Serve as the Army's principal liaison representative to Federal, state, and local law enforcement agencies to exchange terrorist related criminal information.

h. Conduct personal security vulnerability assessments (PSVAs) for all personnel designated by MACOM commanders and other Level I HRPs as directed by HQDA. Provide technical assistance to local Provost Marshals during the conduct of PSVAs for Level II HRP.

i. Establish procedures to ensure appropriate liaison at all levels between USACIDC and INSCOM elements operating in support of the CBT/T Program.

2–12. Commanding General, U.S. Army Intelligence and Security Command (CG, INSCOM)

The CG, INSCOM will—

a. Conduct foreign intelligence (FI) and counterintelligence (CI) activities to collect and disseminate information on all aspects of terrorism and terrorist threats against the Army and DoD. These activities will be conducted per applicable Army regulations.

b. Maintain a full-time capability to report and disseminate INSCOM-collected, time-sensitive information concerning the terrorist threat against Army personnel, facilities and other assets.

c. Provide supported Army commanders with information concerning the terrorist threat against their personnel, facilities and operations.

d. Include terrorist threat information in briefings on subversion and espionage directed against the Army (SAEDA) per AR 381–12.

e. Serve as the Army's intelligence liaison representative to Federal, State, and local agencies and host country federal, state, and local level agencies to exchange terrorism information. Host country coordination should be per agreements between the Theater Army Commander and other U.S. agencies.

f. Analyze information on all aspects of terrorism and the threat it poses to U.S. Army personnel, facilities and activities.

g. Provide terrorism analyses and threat assessments in response to Army Staff requirements.

h. Serve as the Army's analytic representative for terrorism intelligence.

i. Coordinate with the CG, USACE to ensure that threat assessments are sufficiently detailed to serve as a basis for design. These assessments should be applicable over the long term and should include terrorist capabilities (tactics, weapons, tools and explosives).

j. Establish procedures to ensure appropriate liaison at all levels between INSCOM and USACIDC elements operating in support of the CBT/T Program.

k. In conjunction with ODCSOPS publish a Monthly International Terrorism Summary (MITS) which provides both unclassified and classified summaries of the terrorist threat in HQDA designated high and potential physical threat countries. Ensure that the MITS is disseminated to all personnel responsible for implementation of DA policies governing administration of threat briefings prior to official and nonofficial travel.

2–13. Commanding General, U.S. Army Corps of Engineers (CG, USACE)

The CG, USACE will—

a. Develop and disseminate CBT/T protective design criteria and standards for Army facilities.

b. Develop and recommend security engineering techniques to deter or reduce the impact of terrorist attacks.

c. Develop requirements and execute programs for research and studies supporting the incorporation of CBT/T initiatives into Army facilities and installations.

d. Coordinate with the CG, INSCOM to ensure threat definition is sufficiently detailed to serve as a basis for design. Such threat definitions should include long term projections of worldwide terrorist capabilities and include a description of likely aggressor tactics, weapons, tools and explosives.

e. Assist, as requested, MACOM and installation commanders in conducting physical security and force protection assessments.

f. Provide training for installation level CBT/T planners, focused on structural measures appropriate for potential terrorist tactics, weapons, tools and explosives.

g. Ensure that USACE engineers have incorporated physical security measures as prescribed by installation commanders.

2–14. Commanding General, U.S. Army Special Operations Command (CG, USASOC)

The CG, USASOC will—

a. Develop doctrine and training required to support execution of AT and CT operations by Army Special Operations.

b. Conduct resident personal protection training for DoD personnel assigned to High Risk Billets.

c. Conduct resident training to prepare officers, noncommissioned officers and equivalent grade civilian employees to train individuals and units in personal protection.

d. Coordinate AT doctrine and training with the Army Specified Functional Proponent for CBT/T.

2–15. Commanding General, Military District of Washington (CG, MDW)

The CG, MDW will coordinate combatting terrorism operations of all the Services within the National Capital Region, per existing inter-Service agreements.

2–16. MACOM Commanders (For purposes of this regulation, MACOM requirements also apply to the commanders of U.S. Army Recruiting Command, U.S. Military Entrance Processing Command, U.S. Army Strategic Defense Command and U.S. Army Central Command.)

MACOM Commanders will—

a. Publish guidance for all subordinate commands concerning implementation of the CBT/T Program, to include command specific guidance concerning implementation of THREATCON measures outlined in appendix B.

b. Establish a MACOM CBT/T or Force Protection Committee, a CBT/T fusion cell per procedures in chapter 3, and appoint a command Force Protection Officer.

c. Ensure compliance with all THREATCON reporting and implementation procedures.

d. Ensure that SAEDA training (AR 381–12) includes information on the nature of the terrorist threat, vulnerabilities of military personnel, civilian employees and their family members to terrorist acts, and self-protection measures that can be employed to thwart such acts.

e. Develop AT education and training programs, threat briefings, and public affairs command information programs to inform and increase antiterrorism and personal protection awareness among military and civilian personnel and their family members. Such materials should be disseminated on a routine basis in overseas locations and during periods when the THREATCON level exceeds NORMAL in CONUS locations.

f. Develop procedures to ensure that personnel traveling to high and potential physical threat countries (on leave, temporary duty (TDY), permanent change of station (PCS), or unit deployments/rotations) are briefed concerning the threat and informed of individual protective measures prior to initiation of travel. (See chap 3.)

g. Ensure that SRT units have the requisite organizational equipment, training, and leadership needed to provide SRT support to subordinate installations, facilities, and activities. Whenever practicable, SRT capability should be provided by a Federal, state or local law enforcement agency or by another Service, per written agreements between the installation and the supporting agency. Where practicable, commanders in OCONUS areas should request SRT support from host nation police agencies. Prior to signing an agreement for SRT support from a civilian or host nation police agency, commanders will assess the capability of that agency to perform the SRT mission per AR 190–58.

h. Review CBT/T operations plans, operations orders, and/or SOPs developed by subordinate commands on an annual basis. Ensure that these plans, orders or SOPs are exercised at installation level on an annual basis per chapter 3.

i. Program funds and identify personnel to attend specialized CBT/T training. Ensure that all personnel with significant CBT/T responsibilities in operations, intelligence, criminal investigation, and Provost Marshal staff sections receive specialized training.

j. Establish a system to monitor expenditure of CBT/T funds from programming through budget execution.

k. Ensure that CBT/T design measures have been considered and included, as appropriate, in the command's construction program per Army policy (AR 415–15). Ensure that recommended protective measures are based on risk and threat analyses.

l. Designate HRP per AR 190–58 and chapter 3. Report such designations to HQDA per chapter 3. (The DAS exercises this authority within the Military District of Washington.)

m. Establish written procedures for disseminating time sensitive threat information during both duty and non-duty hours. Ensure that subordinate commands, to company (or equivalent) level, have developed supporting procedures.

n. Approve, in writing, the internal establishment of full-time Protective Service organizations within their commands.

2–17. State Adjutants General

Adjutants General will—

a. Publish guidance for all subordinate commands concerning implementation of the CBT/T Program, to include State specific guidance concerning implementation of THREATCON measures outlined in appendix B.

b. Establish a State CBT/T or Force Protection Committee and a CBT/T fusion cell per procedures in chapter 3.

c. Ensure compliance with all THREATCON reporting and implementation procedures. OCONUS Adjutants General will report changes in their THREATCON to the MACOM responsible for the geographic area.

d. Develop procedures to ensure that personnel traveling to high and potential physical threat countries (on leave, TDY, PCS, or unit deployments) are briefed concerning the threat and informed of individual protective measures prior to initiation of travel. (see chapter 3)

e. Ensure that security plans and SOPs developed by subordinate units address antiterrorism protective measures and responses to terrorist acts. In addition, ensure that the senior commander at each Armory location has coordinated procedures for responding to terrorist acts with the supporting FBI office and with local law enforcement agencies.

f. Program funds and identify personnel to attend specialized CBT/T training.

g. Establish a system to monitor expenditure of CBT/T funds from programming through budget execution.

h. Ensure that CBT/T design measures have been considered and included, as appropriate, in construction projects. In addition, ensure that recommended protective measures are based on risk and threat analyses.

i. Designate HRP per AR 190–58, chapter 3 and the following guidelines—

(1) State Adjutants General are authorized to designate personnel as Level I HRP. Commander, Forces Command, or Commander, USARPAC, as appropriate, will be provided written notice of such designations.

(2) The authority to designate Level II HRP rests with Adjutants General and cannot be further delegated.

j. Report personnel designated as HRP level I to HQDA per chapter 3.

k. Establish written procedures for disseminating time sensitive threat information during both duty and non-duty hours. Ensure that subordinate commands, to company (or equivalent) level, have developed supporting procedures.

2–18. Installation Commanders (For purposes of this regulation, installation requirements also apply to the U.S. Military Academy.)

Government owned contractor operated facilities not able to support the requirements below will forward a request to the next higher headquarters for support. Installation Commanders will—

a. Establish an installation CBT/T or Force Protection Committee and a CBT/T fusion cell per procedures in chapter 3, and appoint a command Force Protection Officer.

b. Designate in writing a prioritized list of mission essential vulnerable areas (MEVAs) and indicate MEVA locations that are likely to be targeted by terrorists and most vulnerable to terrorist attacks (these locations may include housing areas, troop billets, schools, chapels and other locations where large numbers of personnel reside or congregate).

c. Develop a comprehensive CBT/T or force protection operations plan or operations order which—

(1) Includes security procedures required at all THREATCON levels (NORMAL through DELTA).

(2) Includes precautions appropriate to deter terrorist attacks against individuals and property.

(3) Is fully coordinated with the supporting FBI office and appropriate state and local law enforcement agencies, or, OCONUS, with host nation security and law enforcement agencies.

(4) Places special emphasis on security of HRP and personnel whose duties require presence outside the Army community.

(5) Describes procedures for responding to terrorist incidents occurring on the installation, facility or activity.

d. Review installation and supporting CBT/T operations plans and orders, and SOPs prepared by subordinate commands and agencies on an annual basis. Retain a written record of such reviews for two years following their completion. Exercise installation level plans, orders and SOPs on an annual basis; retain exercise results and lessons learned for two years following completion of the exercise.

e. Prepare an installation/local security threat assessment that describes the current terrorist threat. Assessments should be prepared at least annually (and updated as required) and form the basis for identifying vulnerabilities that require correction.

f. Ensure that personnel with significant CBT/T responsibilities in operations, intelligence and Provost Marshal staff sections have received appropriate specialized training.

g. Ensure that CBT/T design measures have been considered and, where appropriate, incorporated in the installation's military construction design program, and ensure that the design is based on risk and threat analyses.

h. Ensure that risk analyses for all new construction projects and renovations of MEVA are performed per procedures outlined in DA PAM 190–51.

i. Establish and implement an installation THREATCON commensurate with the terrorist threat, existing vulnerabilities and additional factors outlined in paragraph 3–6b of this regulation.

j. Ensure that SAEDA training (AR 381–12) includes information on the nature of the terrorist threat, vulnerabilities of personnel and their families to terrorist acts, and self-protection measures that can be employed to deter or defeat such acts.

k. Develop and administer AT education and training programs, threat briefings, and public affairs command information programs to inform and increase antiterrorism and personal protection awareness among military and civilian personnel and their family members. Such materials should be disseminated on a routine basis in overseas areas and during periods when the THREATCON level exceeds NORMAL in CONUS locations.

l. Organize, train, equip and evaluate an SRT using existing resources or coordinate with a civilian or host nation law enforcement agency, or with another military installation, to provide such capability, when per Federal law and guidance from higher headquarters. Commanders will ensure that supporting civilian and host nation SRT units have the requisite organization, equipment and training.

m. Establish a system to monitor expenditure of CBT/T funds from programming through budget execution.

n. Establish written procedures for dissemination of time-sensitive threat information during both duty and non-duty hours. Ensure that subordinate commands, through company (or equivalent) level, have developed supporting procedures.

o. Develop procedures to ensure that all U.S. Army personnel (military and civilian) traveling in high or potential physical threat countries (on leave, temporary duty (TDY), permanent change of station (PCS), or unit deployments/rotations) are briefed concerning the threat and informed of individual protective measures prior to initiation of travel. (See chap 3.)

p. Incorporate installation physical security initiatives into the Installation Master Plan. These initiatives should support the following objectives:

(1) Reduce installation/facility vulnerabilities in a manner that deters terrorist attack.

(2) Reduce physical security program costs.

(3) Inspire an appropriate level of confidence in the commander's ability to protect personnel and assets.

2–19. Commanders of deployed corps, divisions, brigades and battalions (which deploy or deploy subordinate elements to OCONUS locations or CONUS locations where a credible terrorist threat exists)

Commanders will—

a. Ensure that SAEDA training (AR 381–12) includes information on the nature of the terrorist threat, vulnerabilities of military personnel and family members to terrorist attacks, and self-protection measures that can be employed to thwart such acts.

b. Develop procedures to ensure that personnel are briefed concerning the threat prior to any deployment/rotation.

c. Ensure that all personnel with significant CBT/T responsibilities in operations, intelligence and Provost Marshal staff sections have received specialized CBT/T training.

d. Establish written procedures for disseminating time sensitive threat information during both duty and non-duty hours. Ensure that subordinate commands, to company level, have developed supporting procedures.

e. Review operations orders and plans for deployments, and supporting SOPs to ensure that they include—

(1) An assessment of the terrorist threat while preparing for movement, during movement and at the final destination.

(2) Specific procedures for protecting personnel, facilities and equipment from terrorist attack.

(3) Specific procedures for reporting and defending against an actual terrorist attack, particularly during deployments and at isolated facilities. Procedures should include action to be taken in response to terrorist demands, threats, or actions by terrorist groups, and security procedures to be executed during routine local travel.

f. Implement the THREATCON system (to include reporting procedures) for all units deployed away from parent organizations.

Chapter 3
Combatting Terrorism Procedures

3–1. CBT/T Planning

a. Planning for CBT/T requires the personal involvement of the commander.

b. All CBT/T staff efforts should be coordinated by the operations officer (DCSOPS, DPTMSEC, G3, S3 or equivalent), working closely with the Provost Marshal, intelligence officer and staff engineer. In those headquarters organized without a separate and distinct operations staff element, the commander will formally assign responsibility for CBT/T to the staff principal whose functions most closely align with the "operations" function.

c. The operations officer should ensure that information management, logistics, medical, SJA, and public affairs officers are involved in CBT/T planning.

3–2. Plans, Orders and Other Implementing Guidance

a. The time to begin detailed planning for responding to a terrorist threat or terrorist attack is before a threat develops or an attack occurs.

b. Commanders at all levels should ensure that CBT/T plans, orders or other implementing guidance are realistic and comprehensive, and that such documents prescribe both preemptive, or defensive measures designed to reduce command vulnerabilities prior to a terrorist attack, and detailed procedures for responding to a terrorist attack after it occurs.

c. Forms of implementing guidance.

(1) MACOM commanders will provide CBT/T implementing guidance to subordinate organizations by publishing a supplement to this regulation (which must be approved by HQDA), or by issuing an operations plan or order. A copy of MACOM implementing guidance will be provided to HQDA (DAMO–ODL–CBT).

(2) State Adjutants General and installation commanders will issue operations plans or orders which provide CBT/T implementing guidance to subordinate organizations. The requirement to develop supporting plans or orders at subordinate levels will be addressed in the plan or order issued by the Adjutant General or installation commander.

(3) All operations plans and orders will contain an assessment of the actual terrorist threat (or absence of threat) in the 'Enemy Forces' paragraph. In addition, the 'Coordinating Instructions' of such plans and orders will prescribe appropriate actions for reporting terrorist threat information, responding to a terrorist attack and reporting terrorist incidents (this requirement can be met by referencing a Standing Operating Procedure or other document that is readily available to all units/organizations responsible for executing the plan or order). Unit movement directives will contain instructions directing a predeployment orientation concerning the terrorist threat if the unit is deploying to a country designated by DoD as a high or potential physical threat country.

(4) All organizations not otherwise required to develop CBT/T plans or orders, or address CBT/T related concerns in other operations plans or orders, will incorporate CBT/T into existing documents (such as Standing Operating Procedures) which prescribe security procedures for the organization. At a minimum, CBT/T guidance incorporated into other policy documents will address specific, detailed procedures for implementing THREATCON measures described in appendix B.

3–3. Combatting Terrorism Committees and Fusion Cells

a. At HQDA, the CBT/T program is formally overseen by a General Officer Steering Committee (GOSC) comprised of a general officer or civilian equivalent from each HQDA staff agency with significant responsibility for some aspect of CBT/T. The GOSC for CBT/T provides a senior level forum for discussion and resolution of Army-wide CBT/T matters, to include overall CBT/T policy and resource allocation. The GOSC for CBT/T is chaired by the Director of Operations, Readiness and Mobilization, ODCSOPS, HQDA, and operates in accordance with DA level policy guidance.

b. CBT/T or Force Protection Committees will be established at MACOM through installation (or equivalent) levels and by State Adjutants General. CBT/T or Force Protection Committees will—

(1) Meet periodically (at least twice annually) to discuss the terrorist threat, asset vulnerabilities and existing CBT/T plans and guidance, assign priorities to funding request, repair, and construction for CBT/T projects.

(2) Operate under the direction of the Chief of Staff or the operations officer (DCSOPS, DPTMSEC, G3, S3 or other individual with key staff responsibility for CBT/T).

(3) Include staff principals (or designated representatives) from each of the following staff sections: Provost Marshal, intelligence engineer, information management, logistics, medical, SJA and public affairs. Other personnel, to include commanders of supporting counterintelligence and CID units, and/or subordinate tenant commanders may be invited at the discretion of the commander.

(4) Provide a written record of meetings to the commander and maintain those records on file for a period of two years.

c. CBT/T fusion cells will be established at MACOM through installation (or installation equivalent) levels, and by State Adjutants General. CBT/T fusion cells will—

(1) Include representation by staff officers with CBT/T responsibilities from operations, Provost Marshal, intelligence and engineer staff sections.

(2) Meet frequently to discuss the current terrorist threat and evaluate security measures that have been implemented or planned for implementation.

(3) Operate under the direction of the command's Force Protection Officer (who is normally assigned to the operations staff section–DCSOPS, DPTMSEC, G3, S3 or equivalent designated section).

(4) Develop issues for presentation to the command's CBT/T or Force Protection Committee.

d. CBT/T committees and fusion cells should meet more frequently during periods of increased terrorist threat. Both groups should form the nucleus of crisis management teams (CMT) constituted to direct emergency operations in response to terrorist threats and terrorist incidents.

☆U.S. GOVERNMENT PRINTING OFFICE: 2002-728-075/60219 A-5 MP 2001